1 Общие замечания

Данный текст представляет из себя краткий конспект лекций по курсу «Математическая логика», рассказанных студентам ИТМО (группы 2537-2539) в 2012-2013 учебном году.

2 Исчисление высказываний

Матлогика — это наука о правильных математических рассуждениях, а поскольку рассуждения обычно ведутся на каком-то языке, то она неразрывна связана с идеей двух языков: *языка исследователя* (или иначе его называют *мета-языком*), и *предметного языка*. Как следует из названий, языком исследователя пользуемся мы, формулируя утверждения или доказывая теоремы о разных способах математических рассуждений, или просто их обсуждая. Сами же математические рассуждения, собственно и составляющие предмет исследования, формализованы в некотором предметном языке.

Мы начнём с очень простого предметного языка — языка исчисления высказываний. Элементами (строками) данного языка являются некоторые выражения (формулы), по структуре очень похожие на арифметические, которые называются *высказываниями*.

Каждое высказывание — это либо *пропозициональная переменная* — большая буква латинского алфавита, возможно, с цифровым индексом, либо оно составлено из одного или двух высказываний меньшего размера, соединённых логической связкой.

Связок в языке мы определим 4 (хотя при необходимости этот список может быть в любой момент изменен).

- конъюнкция: если $\alpha\beta$ — высказывания, то $\alpha\&\beta$ — тоже высказывание.
- дизъюнкция: если $\alpha\beta$ — высказывания, то $\alpha \vee \beta$ — тоже высказывание.
- импликация: если $\alpha\beta$ — высказывания, то $\alpha \to \beta$ — тоже высказывание.
- отрицание: если α — высказывание, то $\neg\alpha$ — тоже высказывание.

Высказывания, подробности которых нас не интересуют, мы будем обозначать начальными буквами греческого алфавита (α, β, γ и т.п.).

2.1 Оценка высказываний

Процесс «вычисления» значения высказываний (*оценка* высказываний) имеет совершенно естественное определение. Мы фиксируем некоторое множество *истинностных значений*, для начала мы в качестве такого множества возьмем множество $\{\text{И}, \text{Л}\}$, здесь И означает истину, а Л — ложь. Всем пропозициональным переменным мы приписываем некоторое значение, а затем рекурсивно вычисляем значение выражения естественным для указанных связок образом.

В дальнейшем мы будем брать необычные множества истинностных значений, и будем давать неожиданный смысл связкам, однако, классическая интерпретация связок является традиционной и всегда подразумевается, если не указано иного.

Среди высказываний выделяются те, что остаются истинными при любой оценке пропозициональных переменных. Такие высказывания называют *тавталогиями* или *общезначимыми высказываниями*. Также, на языке исследователя общезначимость высказывания α можно кратко записать как $\models \alpha$.

Оценку высказываний мы будем записывать с помощью двойных квадратных скобок. Например, нетрудно видеть, что $[\![P \to P]\!] = \text{И}$. Если нам требуется явно задать значения некоторых пропозициональных переменных, мы будем записывать эти значения как верхний индекс: $[\![P \to Q]\!]^{P:=\text{Л}} = \text{И}$.

2.2 Доказательства

В любой теории есть некоторые утверждения (аксиомы), которые принимаются без доказательства. В исчислении высказываний мы должны явно определить список всех возможных аксиом. Например, мы можем взять утверждение $A\&B \to A$ в качестве аксиомы. Однако, у него есть множество аналогичных утверждений, например, $B\&A \to B$, которые не отличаясь по сути, отличаются по записи, и формально говоря, являются другим утверждением.

Для решения вопроса мы введём понятие *схемы аксиом* — некоторого обобщённого шаблона, подставляя значения в который, мы получаем различные, но схожие аксиомы. Например, схема аксиом $\psi\&\phi \to \psi$ позволяет получить как аксиому $A\&B \to A$ (при подстановке $\psi := A, \phi := B$), так и аксиому $B\&A \to B$.

Возьмем следующие схемы аксиом для исчисления высказываний.

(1) $(\phi) \to ((\psi) \to (\phi))$
(2) $((\phi) \to (\psi)) \to ((\phi) \to (\psi) \to (\pi)) \to ((\phi) \to (\pi))$
(3) $(\phi) \to (\psi) \to (\phi)\&(\psi)$
(4) $(\phi)\&(\psi) \to (\phi)$
(5) $(\phi)\&(\psi) \to (\psi)$
(6) $(\phi) \to (\phi) \vee (\psi)$
(7) $(\psi) \to (\phi) \vee (\psi)$
(8) $((\phi) \to (\pi)) \to ((\psi) \to (\pi)) \to ((\phi) \vee (\psi) \to (\pi))$
(9) $((\phi) \to (\psi)) \to ((\phi) \to \neg(\psi)) \to \neg(\phi)$
(10) $\neg\neg(\phi) \to (\phi)$

Помимо аксиом, нам требуется каким-то образом научиться преобразовывать одни верные утверждения в другие. Сделаем это с помощью правил вывода. У нас пока будет одно правило вывода — Modus Ponens. Это также схема, она позволяет при доказанности двух формул ψ и $\psi \to \phi$ считать доказанной формулу ϕ.

Определение 2.1. *Доказательство* в исчислении высказываний — это некоторая конечная последовательность выражений $\alpha_1, \alpha_2 \ldots \alpha_n$ из языка L, такая, что каждое из утверждений $\alpha_i (1 \le i \le n)$ либо является аксиомой, либо получается из других утверждений $\alpha_{P_1}, \alpha_{P_2} \ldots \alpha_{P_k}$ $(P_1 \ldots P_k < i)$ по правилу вывода.

Определение 2.2. Высказывание α называется доказуемым, если существует доказательство $\alpha_1, \alpha_2 \ldots \alpha_k$, и в нем α_k совпадает с α.

Вообще, схемы аксиом и правила вывода существуют для удобства задания исчисления. В дальнейшем будет очень неудобно возиться с этими объектами. Поэтому мы считаем, что в исчислении имеется бесконечно много аксиом и правил вывода, которые порождаются подстановкой всех возможных формул вместо параметров в схемы.

В качестве сокращения записи в языке исследователя мы будем писать $\vdash \alpha$, чтобы сказать, что α доказуемо.

Традиционно правила вывода записывают так:

$$\frac{\phi \quad (\phi) \to (\psi)}{\psi}$$

3 Теорема о дедукции

Соглашение об обозначениях. Будем обозначать буквами $\Gamma, \Delta, \Sigma, \Pi$ списки формул (возможно, пустые).

Определение 3.1. Вывод из допущений. Пусть Γ – некоторый список высказываний, а α — некоторое высказывание. Тогда мы будем говорить, что высказываение α *выводимо* из Γ (и записывать это как $\Gamma \vdash \alpha$), если существует такая последовательность высказываний $\alpha_1, \alpha_2, \ldots \alpha_{n-1}, \alpha$ (называемая *выводом* α из Γ), что каждое из высказываний α_i — это

- либо аксиома,
- либо получается по правилу Modus Ponens из предыдущих высказываний,
- либо — высказывание из списка Γ.

Элементы Γ мы будем называть *допущениями*. Также эти элементы называют предположениями или гипотезами.

В свете данного определения можно заметить, что доказательство — это вывод из пустого списка допущений.

Теорема 3.1. Теорема о дедукции. Утверждение $\Gamma \vdash \alpha \to \beta$ справедливо тогда и только тогда, когда справедливо, что $\Gamma, \alpha \vdash \beta$.

Для доказательства рассмотрим следующую лемму:

Лемма 3.2. $\vdash \alpha \to \alpha$

Доказательство.

(1)	$\alpha \to (\alpha \to \alpha)$	Сх. акс. 1
(2)	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	Сх. акс. 2
(3)	$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	M.P. 1,2
(4)	$(\alpha \to ((\alpha \to \alpha) \to \alpha))$	Сх. акс. 1
(5)	$\alpha \to \alpha$	M.P. 4,3

□

Доказательство теоремы 3.1. Сперва докажем прямое следствие. Для этого нам достаточно научиться по любому выводу $\alpha \to \beta$ из Γ строить вывод β из Γ, α. Возьмем вывод формулы $\alpha \to \beta$, то есть некоторую последовательность формул $\delta_1 \ldots \delta_{m-1}; \alpha \to \beta$. Добавив к выводу 2 формулы, получаем требуемый вывод:

(1)	δ_1	
	$\ldots$	
$(m-1)$	δ_{m-1}	
(m)	$\alpha \to \beta$	
$(m+1)$	α	«Свежедобавленная» аксиома
$(m+2)$	β	M.P. m, $m+1$

Теперь докажем обратное. Нам необходимо построить вывод утверждения $\Gamma \vdash \alpha \to \beta$ по имеющемуся выводу $\delta_1 \ldots \delta_{m-1}, \beta$. Мы поступим так: сперва набросаем план вывода – разместим по тексту «ключевые» формулы, которые потом дополним до полноценного вывода промежуточными формулами.

План вывода будет такой:

(1)	$\Gamma \vdash \alpha \to \delta_1$
$\ldots$	
$(m-1)$	$\Gamma \vdash \alpha \to \delta_{m-1}$
(m)	$\Gamma \vdash \alpha \to \beta$

Теперь надо дополнить его до полноценного вывода. Будем рассматривать формулы подряд и перед каждой формулой добавлять некоторое количество формул, обосновывающих соответствующий шаг доказательства. Рассмотрим формулу номер i. Возможны следующие варианты:

1. δ_i — это аксиома или предположение, входящее в Γ. Тогда перед этой формулой вставим формулы δ_i и $\delta_i \to (\alpha \to \delta_i)$, и окажется, что i-я формула выводится из предыдущих двух формул путем применения правила Modus Ponens.

2. δ_i совпадает с α. Тогда мы вставим перед ней 4 первые формулы из леммы, и $\delta_i \to \alpha$ будет получаться по правилу Modus Ponens.

3. δ_i выводится по правилу Modus Ponens из каких-то других утверждений δ_j и δ_k (при этом $\delta_k \equiv \delta_j \to \delta_i$), где $j < i$ и $k < i$. Покажем, что $\alpha \to \delta_i$ тоже может быть выведена из утверждений $\alpha \to \delta_j$ и $\alpha \to (\delta_j \to \delta_i)$.

   Для этого добавим два высказывания:

$(\alpha \to \delta_j) \to ((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	Сх. акс. 2
$((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	М.Р. из j и $i-6$

□

По аналогии мы можем рассмотреть отношение *следования*. Будем говорить, что высказывание α следует из высказываний Γ, если при любой оценке пропозициональных переменных, входящих в высказывания Γ и α, на которых все высказывания из Γ истинны, α также истинно. Записывать, что α следует из Γ, будем так: $\Gamma \models \alpha$.

4 Теорема о полноте исчисления высказываний

Определение 4.1. Введем обозначение. Пусть α — это некоторое высказывание, а x — некоторое истинностное значение. Тогда обозначим за ${}_{[x]}\alpha$ высказывание α, если x — истина, и $\neg(\alpha)$, если x — ложь. Также, если формула α — это формула с n пропозициональными переменными $P_1 \dots P_n$, и $x_1 \dots x_n$ — некоторые истинностные значения, то за $[\![\alpha]\!]^{P_1:=x_1,\dots P_n:=x_n}$ обозначим значение формулы α при подстановке значений $x_1 \dots x_n$ вместо переменных $P_1 \dots P_n$.

Лемма 4.1. Если $\Gamma, \Sigma \vdash \alpha$, то $\Gamma, \Delta, \Sigma \vdash \alpha$. Если $\Gamma, \Delta, \Sigma, \Pi \vdash \alpha$, то $\Gamma, \Sigma, \Delta, \Pi \vdash \alpha$.

Доказательство. Упражнение □

Лемма 4.2. Если справедливы 3 утверждения: $\Gamma \vdash \gamma$, $\Delta \vdash \delta$ и $\gamma, \delta \vdash \alpha$, то справедливо и $\Gamma, \Delta \vdash \alpha$

Доказательство. Мы получим требуемый вывод, просто последовательно соединив все три исходных вывода. Первые два вывода будут (очевидно) корретными при допущениях Γ и Δ. В третьем же выводе могут использоваться высказывания γ и δ, отсутствующие в предположениях. Но поскольку эти высказывания доказаны в первых двух частях вывода, мы будем иметь полное право их упоминать — на тех же основаниях, на которых они указаны в конце соответствующих доказательств.

□

Возьмем некоторую связку исчисления высказываний, например конъюнкцию: $A\&B$. Построим для нее таблицу истинности. По каждой строчке построим утверждение, в котором отрицания появляются там, где в таблице истинности находится *Л*:

A	B	$A\&B$	утверждение
Л	Л	Л	$\neg A, \neg B \vdash \neg(A\&B)$
Л	И	Л	$\neg A, B \vdash \neg(A\&B)$
И	Л	Л	$A, \neg B \vdash \neg(A\&B)$
И	И	И	$A, B \vdash A\&B$

Лемма 4.3. Каждое из построенных по таблицам истинности утверждений доказуемо.

Доказательство. Упражнение. □

Лемма 4.4 (Правило контрапозиции)**.** Каковы бы ни были формулы α и β, справедливо, что $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

Доказательство. Сперва докажем, что $\alpha \to \beta, \neg\beta \vdash \neg\alpha$.

(1)	$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$	Сх. акс. 8
(2)	$\alpha \to \beta$	Допущение
(3)	$(\alpha \to \neg\beta) \to \neg\alpha$	М.Р. 2,1
(4)	$\neg\beta \to (\alpha \to \neg\beta)$	Сх. акс. 1
(5)	$\neg\beta$	Допущение
(6)	$\alpha \to \neg\beta$	М.Р. 5,4
(7)	$\neg\alpha$	М.Р. 6,3

Тогда, применив 2 раза Теорему о дедукции, получим вывод требуемого утверждения. □

Лемма 4.5. Правило исключенного третьего. Какова бы ни была формула α, $\vdash \alpha \vee \neg\alpha$

Доказательство. Доказательство проведем в 3 этапа.

1. Для начала покажем $\vdash \neg(\alpha \vee \neg\alpha) \to \neg\alpha$:

(1)	$\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 6
$(2) \dots (n+1)$	$\gamma_1, \dots \gamma_{n-1}, (\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\alpha)$	Д-во из леммы 4.4
$(n+2)$	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	М.Р. $1, n+1$

2. Затем докажем $\vdash \neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$:

(1)	$\neg\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 7
$(2) \dots (k+1)$	$\delta_1, \dots \delta_{k-1}, (\neg\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha)$	Д-во из леммы 4.4
$(k+2)$	$\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$	М.Р. $1, k+1$

3. Теперь докажем все вместе:

(1)	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	по пункту 1
(2)	$\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$	по пункту 2
(3)	$(\neg(\alpha \vee \neg\alpha) \to \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha) \to (\neg\neg(\alpha \vee \neg\alpha))$	Сх. акс. 9
(4)	$(\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha) \to \neg\neg(\alpha \vee \neg\alpha)$	М.Р. 1,3
(5)	$\neg\neg(\alpha \vee \neg\alpha)$	М.Р. 2,4
(6)	$\neg\neg(\alpha \vee \neg\alpha) \to (\alpha \vee \neg\alpha)$	Сх. акс. 10
(7)	$\alpha \vee \neg\alpha$	М.Р. 5,6

□

Лемма 4.6. Об исключении допущения. Пусть справедливо $\Gamma, \rho \vdash \alpha$ и $\Gamma, \neg\rho \vdash \alpha$. Тогда также справедливо $\Gamma \vdash \alpha$.

Доказательство. Применив теорему о дедукции к условиям теоремы получим следующее:

$\Gamma \vdash \rho \to \alpha$

$\Gamma \vdash \neg\rho \to \alpha$

Тогда следующий вывод покажет $\Gamma \vdash \alpha$:

$(1) \dots (p)$	$\gamma_1, \dots \gamma_{p-1}, \rho \to \alpha$	Вывод $\Gamma \vdash \rho \to \alpha$
$(p+1) \dots (q)$	$\delta_1, \dots \delta_{q-p-1}, \neg\rho \to \alpha$	Вывод $\Gamma \vdash \neg\rho \to \alpha$
$(q+1) \dots (r)$	$\epsilon_1, \dots \epsilon_{r-q-1}, \rho \vee \neg\rho$	Лемма 4.5
$(r+1)$	$(\rho \to \alpha) \to (\neg\rho \to \alpha) \to (\rho \vee \neg\rho) \to \alpha$	Сх. аксиом 8
$(r+2)$	$(\neg\rho \to \alpha) \to (\rho \vee \neg\rho \to \alpha)$	М.Р. 1, $r+1$
$(r+3)$	$\rho \vee \neg\rho \to \alpha$	М.Р. p, $r+2$
$(r+4)$	α	М.Р. r, $r+3$

□

Теорема 4.7. О полноте исчисления высказываний. Пусть справедливо $\models \alpha$. Тогда также справедливо, что $\vdash \alpha$.

Доказательство. Для доказательства теоремы мы докажем чуть более сильное утверждение — что для любого k от 0 до n и любой оценки переменных $x_1, \dots x_k$ справедливо ${}_{[x_1]}P_1, \dots {}_{[x_k]}P_k \vdash \alpha$. Нетрудно заметить, что утверждение теоремы непосредственно следует из данного утверждения для $k = 0$. Доказательство будет вестись индукцией по $n - k$.

База. Пусть $n - k = 0$, то есть $k = n$. $\models \alpha$ означает, что при любой оценке $x_1, \dots x_n$ пропозициональных переменных $P_1, \dots P_n$ справедливо $\alpha[P_1 := x_1, \dots P_n := x_n] = \text{И}$. Возьмем некоторую оценку переменных $x_1, \dots x_n$. Тогда, по лемме 4, ${}_{[x_1]}P_1, \dots {}_{[x_n]}P_n \vdash {}_{\alpha[P_1:=x_1,\dots P_n:=x_n]}\alpha$ то есть ${}_{[x_1]}P_1, \dots {}_{[x_n]}P_n \vdash \alpha$.

Переход. Пусть утверждение уже доказано для некоторого $n - k > 0$, покажем его для $n - k + 1$ (то есть доказано для $k < n$, покажем его для $k - 1$). Возьмем некоторую оценку переменных $x_1, \dots x_{k-1}$. По предположению, ${}_{[x_1]}P_1, \dots {}_{[x_k]}P_k \vdash \alpha$, то есть

${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1}, \neg P_k \vdash \alpha$

${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1}, P_k \vdash \alpha$

Тогда по лемме об исключении допущения, справедливо ${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1} \vdash \alpha$.

□

Теорема 4.8. О корректности исчисления высказываний. Пусть справедливо $\vdash \alpha$. Тогда также справедливо, что $\models \alpha$.

Доказательство. По условию теоремы, у нас есть доказательство высказывания α, то есть последовательность высказываний $\alpha_1, \dots \alpha_m$. Каждое высказывание — это либо аксиома, либо применение правила Modus Ponens. Докажем, что для каждого k все высказывания α_l при $l \leq k$ — тавтологии. Доказательство будем вести индукцией по k.

База. Пусть $k = 0$, тогда нет ни одного высказывания, про которое нужно доказать, что оно — тавтология, то есть утверждение автоматически верно.

Переход. Пусть для некоторого k утверждение справедливо, докажем его для $k + 1$. Выберем некоторую оценку $x_1, \dots x_n$ пропозициональных переменных $P_1, \dots P_n$, использованных в высказываниях $\alpha_1 \dots \alpha_{k+1}$. Рассмотрим случаи.

Пусть α_{k+1} — аксиома. В данную аксиому входят одна, две или три формулы $\beta_1, \beta_2, \beta_3$. Подставив всех возможных истинностных значений вместо данных формул можно проверить, что все аксиомы являются тавтологиями, значит, они будут истинны и на тех конкретных значениях, которые примут данные формулы после подстановки значений $x_1, \dots x_n$.

Пусть α_{k+1} получается по правилу Modus Ponens из α_p и α_q, причем $\alpha_q \equiv \alpha_p \to \alpha_{k+1}$. Тогда $[\![\alpha_p]\!]^{P_1:=x_1,\dots P_n:=x_n} = \text{И}$ и $[\![\alpha_p \to \alpha_{k+1}]\!]^{P_1:=x_1,\dots P_n:=x_n} = \text{И}$. Из таблицы истинности импликации следует, что неизбежно $[\![\alpha_{k+1}]\!]^{P_1:=x_1,\dots P_n:=x_n} = \text{И}$.

□

Заметим, что вместе из этих двух теорем следует, что если неверно, что $\vdash \alpha$, то неизбежно найдется контрпример.

5 Интуиционистское исчисление высказываний

Заменим аксиому устранения двойного отрицания на $\phi \to \neg\phi \to \psi$. Полученная система называется интуиционистским исчислением высказываний.

Теорема 5.1. В интуиционистском исчислении высказываний невозможно доказать правило исключенного третьего: $P \vee \neg P$.

Мы рассмотрим *модельное* доказательство. То есть, мы построим некоторую модель для исчисления высказываний — так определим истинностные значения и связки, что в нем правило исключенного третьего перестанет быть тавтологией, при этом построенная нами модель останется корректной.

Пусть множество истинностных значений будет состоять из трех элементов: И, Н и Л. Определим отношение порядка, будем считать, что И $>$ Н $>$ Л.

Все связки на истине и лжи действуют традиционно, необходимо описать только их поведение с элементом Н. Для двух операций дадим естественные обобщения. $A\&B = min(A, B)$, $A \vee B = max(A, B)$. Однако, положим $\neg$Н $=$ Л. Также, операцию $A \to B$ положим $\neg A \vee B$, за исключением Н $\to$ Н $=$ И

Будем считать, что высказывание истинно на некоторой оценке, если оно на ней принимает значение И. Общезначимость же ($\models \alpha$) означает, что $\alpha[x_1, \dots x_n] =$ И для любой оценки переменных $x_1, \dots x_n$.

Нетрудно показать, что так определенная модель исчисления является корректной — то есть любое утверждение, имеющее доказательство, является тавтологией в смысле данной модели.

Доказательство теоремы 5.1. Поскольку Н $\vee \neg$Н $=$ Н, то в данной модели неверно $\models P \vee \neg P$. Значит, если бы существовало доказательство этого утверждения, то рассмотренная модель была бы некорректной. Значит, для интуиционистского исчисления высказываний неверно $\vdash P \vee \neg P$. □

Однако, так построенная логика (с такой моделью) не является полной. Например, высказывание $\neg P \vee \neg\neg P$, не являющееся доказуемым в интуиционистской логике, тем не менее оказывается истинным. Сейчас мы рассмотрим другие модели, обладающие свойством полноты.

5.1 Топологическая интерпретация интуиционистского исчисления высказываний

Пусть дано некоторое исчисление высказываний, для которого нам нужно построить модель — предложить способ оценки истинности выражений. Начинаем мы с множества истинностных значений. Возьмем в качестве этого множества все открытые множества некоторого заранее выбранного топологического пространства. Определим оценку для связок интуиционистского исчисления высказываний следующим образом:

$$[\![A\&B]\!] = [\![A]\!] \cap [\![B]\!]$$
$$[\![A \vee B]\!] = [\![A]\!] \cup [\![B]\!]$$
$$[\![A \to B]\!] = (c[\![A]\!] \cup [\![B]\!])^\circ$$
$$[\![\neg A]\!] = (c[\![A]\!])^\circ$$

Будем считать, что формула истинна в данной модели, если её значение оказалось равно всему пространству.

Например, возьмем в качестве пространства $\mathbb{R}$, и вычислим значение формулы $A \vee \neg A$ при A равном $(0,1)$: $[\![A \vee \neg A]\!] = (0,1) \cup [\![\neg A]\!] = (0,1) \cup (c(0,1))^\circ = (0,1) \cup ((-\infty, 0) \cup (1, \infty)) = (-\infty, 0) \cup (0,1) \cup (1, \infty)$. Нетрудно видеть, что данная формула оказалась не общезначимой в данной интерпретации.

5.2 Модели Крипке

См. Шень, Верещагин

6 Исчисление предикатов

Выберем множество истинностных значений V. Также, выберем некоторое предметное множество D. *n-местным предикатом* мы назовем функцию из D^n в V. Как и раньше, мы ограничимся классическим множеством V – истина и ложь, но оставляем потенциальную возможность его расширить.

Предикаты могут быть 0-местными, в этом случае это хорошо нам известные пропозициональные переменные, принимающие какие-то истинностные значения, в происхождение которых мы не вникаем.

Рассмотрим следующий известный пример: каждый человек смертен, Сократ - человек, следовательно, Сократ - смертен. Мы можем формализовать это выражение с помощью предикатов: множество D - это будет множество всех существ, $S(x)$ - предикат «быть смертным», $H(x)$ - предикат «быть человеком». Тогда фраза в полу-формальном виде выглядит так: Для каждого x, такого, что $H(x)$ верно $S(x)$, поэтому поскольку H(Сократ), значит, что имеет место S(Сократ).

Определим язык исчисления предикатов более точно. В исчислении предикатов появляется два типа значений: логические (которые участвуют в связках) и предметные (со значениями из множества D). Соответственно, все выражения также делятся на два типа.

Логические выражения — это логические связки плюс предикаты — обобщение пропозициональных переменных, которые теперь могут иметь параметрами предметные выражения.

Предметные выражения — это либо *предметные переменные* (обозначаются маленькими латинскими буквами, также возможно с индексами), либо *функции*, которые действуют из D^n в D.

Например, в выражении $1 + 5 = 0$, понимаемом в смысле исчисления предикатов, есть три константы (то есть, три нуль-местных функции — это 0,1 и 5), одна двухместная функция (плюс), и один предикат (равенство).

Формула исчисления предикатов — это всегда логическое выражение. Например, $5 + 1$ в смысле предыдущего примера не может являться формулой исчисления предикатов.

Помимо этого, мы добавим две новых логических связки:

- Квантор всеобщности: $\forall x \alpha$ (здесь и в следующем определении x — некоторая предметная переменная, а α — некоторая формула исчисления предикатов).
- Квантор существования: $\exists x \alpha$.

Кванторы ведут себя как унарные операции и действуют только на ближайшее за ними выражение логического типа. Например, формула $\forall x x = 5 \vee x = 7$ соответствует формуле $(\forall x(x = 5)) \vee (x = 7)$.

Мы надеемся, что в целом смысл этих конструкций интуитивно понятен, теперь мы перейдем к более формальному описанию.

6.1 Доказательства в исчислении предикатов

Определение 6.1. Дана некоторая формула s. Будем говорить, что подстрока s_1 строки s является подформулой, если она в точности соответствует какому-то одному нетерминалу в дереве разбора строки s.

Определение 6.2. Если в формулу входит подформула, полученная по правилам для кванторов (то есть, $\forall x \alpha$ или $\exists x \alpha$), то мы будем говорить, что формула α находится в области действия данного квантора по переменной x. Также, будем говорить, что любая подформула формулы α находится в области действия данного квантора.

Определение 6.3. Если некоторое вхождение переменной x находится в области действия квантора по переменной x, то такое вхождение мы назовем *связанным*. Вхождение переменной x непосредственно рядом с квантором $(\forall x \dots)$ мы назовем *связывающим*. Те вхождения переменных, которые не являются связанными или связывающими, назовем *свободными*. Формула, не имеющая свободных вхождений переменных, называется *замкнутой*.

Определение 6.4. Будем говорить, что переменная y свободна для x при подстановке в формулу ψ (или просто свободна для подстановки вместо x), если после подстановки y вместо свободных вхождений x ни одно ее вхождение не станет связанным.

Чтобы получить список аксиом для исчисления предикатов, возьмем все схемы аксиом исчисления высказываний и дополним их следующими двумя схемами. Здесь x - переменная, ψ - некоторая формула, y - некоторая переменная. Запись $\psi[x := y]$ будет означать результат подстановки y в ψ вместо всех свободных вхождений x. Пусть y свободно для подстановки вместо x.

(11) $\forall x(\psi) \to (\psi[x := \alpha])$

(12) $(\psi[x := \alpha]) \to \exists x(\psi)$

Заметим, что если взять формулу $\exists x A(x, y)$, то по схеме аксиом (11), если игнорировать ограничение на свободу для подстановки, следующее утверждение должно быть тавталогией: $\forall y \exists x A(x, y) \to \exists x A(x, x)$. Однако, оно ей не является.

Все аксиомы, порожденные данными схемами в новом языке, мы назовем аксиомами исчисления предикатов.

Правила вывода. Пусть x не входит свободно в ϕ. Тогда рассмотрим следующие дополнительные правила вывода исчисления предикатов:

$$\frac{(\phi) \to (\psi)}{(\phi) \to \forall x(\psi)} \quad \frac{(\psi) \to (\phi)}{\exists x(\psi) \to (\phi)}$$

Добавив эти схемы к схеме для правила Modus ponens исчисления высказываний, мы сможем породить множество правил вывода.

6.2 Оценка выражений в исчислении предикатов

Для задания оценки для выражения в исчислении предикатов необходимо вместо оценки для переменных f_P в исчислении высказываний ввести оценку для предикатов: для каждого k-местного предиката P_n^k определить функцию $f_{P_n^k} : D^k \to V$.

Определение 6.5. Формула в исчислении предикатов общезначима, если она истинна на любом предметном множестве D, при любой оценке предикатов, и при любых оценках свободных индивидных переменных.

Определение 6.6. Пусть имеется некоторое исчисление предикатов с множеством аксиом A, и пусть дан некоторый (возможно, пустой) список Γ формул исчисления предикатов. Тогда, вывод формулы α в исчислении с аксиомами $A \cup \Gamma$ мы назовем выводом из допущений Γ, и будем записывать это как $\Gamma \vdash \alpha$.

Формулы в списке формул не обязаны быть замкнутыми: например, легко показать, что $P(x, y), P(x, y) \to P(y, x) \vdash P(y, x)$. Однако, со свободными переменными в допущениях надо быть осторожными, что находит своё отражение в теореме о дедукции для исчисления предикатов.

Теорема 6.1. Теорема о дедукции. Если $\Gamma, \alpha \vdash \beta$, и в доказательстве отстутствуют применения правил для кванторов, использующих свободные переменные из формулы α, то $\Gamma \vdash \alpha \to \beta$

Доказательство. Доказательство разбором случаев. 3 старых случая те же, добавилось 2 новых правила вывода. Упражнение. □

Лемма 6.2. $[\![\psi]\!]^{x:=[\![\theta]\!]} = [\![\psi[x := \theta]]\!]$, если θ свободна для подстановки в ψ вместо x.

Доказательство. Воспользуемся структурной индукцией по выражению ψ.

База индукции. Пусть ψ — это предикат. Тогда из способа вычисления значения предикатов очевидно, что $[\![P(\theta, y_1, \dots y_n)]\!] = [\![P(x, y_1, \dots y_n)]\!]^{x:=[\![\theta]\!]}$.

Переход индукции. Пусть ψ составлено из одного или двух выражений, про которые утверждение уже доказано. Рассмотрим варианты:

- $\psi \equiv \alpha \to \beta$, $\psi \equiv \alpha\&\beta$, $\psi \equiv \alpha \vee \beta$ или $\psi \equiv \neg\alpha$. Рассмотрение всех этих случаев схоже, возьмем для примера конъюнкцию.

  $[\![\alpha\&\beta]\!]^{x:=[\![\theta]\!]} = [\![\alpha]\!]^{x:=[\![\theta]\!]}\&[\![\beta]\!]^{x:=[\![\theta]\!]} = [\![\alpha[x := \theta]]\!]\&[\![\beta[x := \theta]]\!] = [\![\alpha[x := \theta]\&\beta[x := \theta]]\!] = [\![(\alpha\&\beta)[x := \theta]]\!]$

- $\psi \equiv \forall y\alpha$ или $\psi \equiv \exists y\alpha$. Опять же, рассмотрение случаев аналогично. Покажем, что $[\![\forall y\alpha]\!]^{x:=[\![\theta]\!]} = [\![(\forall y\alpha)[x := \theta]]\!]$.

  Без уменьшения общности можем предположить, что x входит свободно в $\forall y\alpha$ — иначе данная замена не оказывает влияние на вычисление результата, и равенство очевидно.

  Поскольку θ свободна для подстановки вместо x в ψ, то, значит, y не входит свободно в θ (иначе свободный y стал бы связанным при подстановке, а подстановки обязательно будут иметь место, раз x входит свободно в $\forall y\alpha$).

  По предположению индукции, $[\![\alpha]\!]^{x:=[\![\theta]\!]} = [\![\alpha[x := \theta]]\!]$. И, более того, $[\![\alpha]\!]^{x:=[\![\theta]\!],y:=v_y} = [\![\alpha[x := \theta]]\!]^{y:=v_y}$, поскольку вычисление оценки θ не зависит от значения переменной y. Значит, оценки полных формул с квантором также будут совпадать.

□

Теорема 6.3. Исчисление предикатов корректно, т.е. любое доказуемое утверждение общезначимо.

Доказательство. Рассмотрим некоторое доказательство $\gamma_1, \dots \gamma_n$, и покажем, что каждое из утверждений в доказательстве является общезначимым. Этим мы покажем утверждение теоремы.

Рассмотрим какое-то утверждение γ_i. Оно либо является частным случаем какой-либо из схем аксиом, либо получено из предыдущих утверждений доказательства. путем применения правил вывода.

Мы ограничимся рассмотрением только новых (по сравнению с исчислением высказываний) схем аксиом и правил, поскольку только в них доказательство будет отличаться от аналогичного для исчисления высказываний.

Возможны следующие варианты:

1. $\gamma_i \equiv \forall x(\psi) \to (\psi[x := \theta])$ при некоторых x (имя переменной тоже может быть разным), ψ и θ. Значит, нам необходимо показать, что при любых x, ψ и θ (естественно, таких, что θ свободна для подстановки вместо x в ψ) данное выражение будет истинным в любой оценке.

   Фиксируем некоторую оценку и докажем утверждение от противного. Пусть это не так, и $[\![\forall x(\psi) \to (\psi[x := \theta])]\!] = \text{Л}$. Тогда неизбежно, что $[\![\forall x(\psi)]\!] = \text{И}$, но $[\![\psi[x := \theta]]\!] = \text{Л}$ (поскольку при остальных значениях подвыражений импликация будет истинна).

Пусть в данной оценке $[\![\theta]\!] = v_\theta$. По лемме 6.2 верно, что $[\![\psi[x := \theta]]\!] = [\![\psi]\!]^{x:=v_\theta}$, причём, поскольку $[\![\psi[x := \theta]]\!] = \text{Л}$, то $[\![\psi]\!]^{x:=v_\theta} = \text{Л}$. Но тогда $[\![\forall x(\psi)]\!] = \text{И}$ означает, что при любом $v_x \in D$ будет выполнено $[\![\psi]\!]^{x:=v_x} = \text{И}$. Противоречие.

2. $\gamma_i \equiv (\psi[x := \theta]) \to \exists x(\psi)$ при некоторых x, ψ и θ. Рассмотрение аналогично предыдущему пункту: заметим, что импликация опровергается только если $[\![\exists x(\psi)]\!] = \text{Л}$, но $[\![\psi[x := \theta]]\!] = \text{И}$. По лемме 6.2 при вычислении оценки формулы мы можем отдельно вычислить $v_\theta = [\![\theta]\!]$, и показать, что $[\![\psi[x := \theta]]\!] = [\![\psi]\!]^{x:=v_\theta}$, что гарантирует существование элемента в D, на котором формула ψ истинна.

3. $\gamma_i \equiv \phi \to \forall x\psi$ и существует такой $j < i$, что $\gamma_j \equiv \phi \to \psi$, при этом x не входит свободно в ϕ.

   Опять же, фиксируем некоторую оценку. Нам нужно показать, что $\forall x\psi$ не бывает ложным, если ϕ истинно.

   По предположению индукции мы знаем, что $[\![\phi \to \psi]\!] = \text{И}$. Пусть $[\![\forall x\psi]\!] = \text{Л}$. То есть, найдётся такой v_x из D, что $[\![\forall x\psi]\!]^{x:=v_x} = \text{Л}$. Но заметим, что x не входит свободно в ϕ. Значит, $[\![\phi]\!]^{x:=v_x} = \text{И}$. Значит, $[\![\phi \to \psi]\!]^{x:=v_x} = \text{Л}$. Противоречие с общезначимостью γ_j.

4. Правило для квантора существования доказывается аналогично.

□

7 Полнота исчисления предикатов

Доказательство этого факта довольно объемно, поэтому мы разделим его на три части.

1. Мы научимся работать с произвольными моделями, уйдя от чрезмерного разнообразия возможных предметных множеств, предикатов и функциональных символов с помощью понятия непротиворечивого множества формул.

2. Мы покажем полноту бесквантворной части исчисления предикатов.

3. Мы сведем полноту исчисления предикатов к полноте бесквантворной его части.

7.1 Непротиворечивое множество формул

Заметим, что само по себе предметное множество в анализе полноты исчисления фигурирует в стороне от главного вопроса. После того, как мы вычислили истинность или ложность конкретных формул в данной модели, мы о конкретном предметном множестве забываем. Соответственно, каждая модель для нашей цели исчерпывающе описывается списком формул, которые в этой модели истинны (в частности, если две разных модели дают одинаковую оценку для каждой из формул — нам нет смысла эти модели разделять). Поэтому мы можем изучать свойства оценок и моделей не прямо, а посредством набора истинных формул. Следующие определения формализуют это понятие.

Определение 7.1. Назовём Γ — множество *замкнутых* формул — непротиворечивым, если ни для какой формулы α невозможно показать, что $\Gamma \vdash \alpha$ и $\Gamma \vdash \neg\alpha$.

Определение 7.2. Полным непротиворечивым множеством (непротиворечивым бесквантворным множеством) формул назвем такое множество Γ, что для любой замкнутой (замкнутой и бесквантворной) формулы α либо $\alpha \in \Gamma$, либо $(\neg\alpha) \in \Gamma$.

Лемма 7.1. Если Γ — непротиворечивое множество формул, то для любой формулы α либо $\Gamma \cup \{\alpha\}$, либо $\Gamma \cup \{\neg\alpha\}$ непротиворечиво.

Доказательство. Пусть это не так, и найдутся такие β и δ, что $\Gamma, \alpha \vdash \beta\&\neg\beta$ и $\Gamma, \neg\alpha \vdash \gamma\&\neg\delta$. Без ограничения общности мы можем предположить, что $\beta \equiv \delta$, поскольку если мы показали $\beta\&\neg\beta$, то мы можем показать и $\delta\&\neg\delta$ (это можно показать на основании доказуемости формулы $\psi \to \neg\psi \to \phi$).

Тогда рассмотрим следующее доказательства в предположении Γ:

$(1 \dots k)$	$\alpha \to \beta\&\neg\beta$	Т. о дедукции
$(k+1 \dots l)$	$\neg\alpha \to \beta\&\neg\beta$	Т. о дедукции
$(l+1)$	$(\alpha \to \beta\&\neg\beta) \to (\neg\alpha \to \beta\&\neg\beta) \to (\alpha \vee \neg\alpha \to \beta\&\neg\beta)$	Сх. акс. 8
$(l+2)$	$(\neg\alpha \to \beta\&\neg\beta) \to (\alpha \vee \neg\alpha \to \beta\&\neg\beta)$	M.P. k,$l+1$
$(l+3)$	$\alpha \vee \neg\alpha \to \beta\&\neg\beta$	M.P. l,$l+2$
$(l+4 \dots m)$	$\alpha \vee \neg\alpha$	Лемма 4.5
$(m+1)$	$\beta\&\neg\beta$	M.P. $l+3$,m

Таким образом, имея доказательства противоречивости Γ, α и $\Gamma, \neg\alpha$, мы можем построить доказательство противоречивости и самого Γ.

□

Теорема 7.2. Любое множество непротиворечивых формул Γ мы можем дополнить до полного (полного бесквантворного) множества.

Доказательство. Упорядочим все возможные формулы (бесквантворные формулы) исчисления (их, как не трудно заметить, счётное количество, и мы можем их занумеровать целыми числами): $\gamma_1, \gamma_2, \ldots$. По данной последовательности построим последовательность множеств $\Gamma_1, \Gamma_2, \ldots$. Положим $\Gamma_1 = \Gamma$. Рассмотрим некоторую формулу γ_n. По предыдущей лемме, либо $\Gamma \cup \{\gamma_n\}$, либо $\Gamma \cup \{\neg\gamma_n\}$ непротиворечиво. Пусть для определенности это $\Gamma \cup \{\gamma_n\}$. Тогда положим $\Gamma_{n+1} = \Gamma_n \cup \{\gamma_n\}$.

Возьмем множество $\Gamma^* = \cup\Gamma_n$. Ясно, что это множество полное — поскольку мы перебрали все формулы и рассматривали каждую формулу вместе со своим отрицанием. Также ясно, что оно непротиворечиво: иначе есть доказательство противоречия (оно, естественно, конечного размера), использующего формулы $\gamma_{p_1} \ldots \gamma_{p_n}$, каждая из которых добавлена на каком-то шаге. Но тогда и множество $\Gamma_{max(p_1,\ldots p_n)+1}$ — множество, построенное при добавлении последней из формул γ_{p_i} — противоречиво, что доказывает утверждение. □

Определение 7.3. Моделью непротиворечивого множества формул мы назовем такие оценки предикатов и функциональных символов, что каждая из формул данного множества истинна. Также, по аналогии с исчислением высказываний, введём обозначение: $\Gamma \models \alpha$ (α следует из Γ), если $[\![\alpha]\!] = \text{И}$ в любой модели множества Γ.

Теорема 7.3. Если $\Gamma \vdash \alpha$, то $\Gamma \models \alpha$.

Доказательство. Механическая проверка всех правил и схем аксиом. □

Теорема 7.4. Если Γ имеет модель, то оно непротиворечиво.

Доказательство. Пусть это не так, то есть $\Gamma \vdash \alpha$ и $\Gamma \vdash \neg\alpha$. Значит, $\Gamma \models \alpha$ и $\Gamma \models \neg\alpha$. То есть, $[\![\alpha]\!] = \text{И}$ Значит, по определению оценки для отрицания, $[\![\neg\alpha]\!] = \text{Л}$. Но это вступает в противоречие с $\Gamma \models \neg\alpha$. □

7.2 Полнота бесквантворной части исчисления предикатов

Лемма 7.5. Пусть Γ — полное непротиворечивое множество бесквантворных формул. Тогда существует модель для Γ.

Доказательство. Будем строить модель, структурной индукцией по сложности формул. Для начала разберемся с предметным множеством. В качестве значений для выражений из констант и функциональных символов зададим строки, содержащие выражения. Например, $[\![c_1]\!] = \text{«}c_1\text{»}$, $[\![f_1(c_1, f_2(c_2))]\!] = \text{«}f_1(c_1, f_2(c_2))\text{»}$ и так далее. Все здесь происходит аналогично тому, как $sin(1)$ есть значение, которое мы не можем вычислить точно и предпочитаем обозначать его своим именем. Таким образом, в множестве D находятся все возможные выражения, составленные из констант и функциональных символов.

Теперь рассмотрим формулу — некоторый предикат вида $\pi \equiv P(\theta_1, \ldots \theta_n)$, где θ_i — это некоторое выражение из функциональных символов и констант (поскольку все формулы замкнуты, в них не могут участвовать переменные). Будем считать его истинным, если $\pi \in \Gamma$ непротиворечиво, иначе, если $\neg\pi \in \Gamma$ будем считать его ложным.

Все связки получат значения естественным образом.

Теперь покажем, что полученная модель действительно является моделью для данного множества формул. Возьмем некоторую формулу γ из Γ. Докажем чуть более сильное свойство: $[\![\gamma]\!] = \text{И}$ тогда и только тогда, когда $\gamma \in \Gamma$.

База. Очевидно, что если атомарная формула принадлежит Γ, то она имеет оценку истина.

Переход. Пусть дана некоторая составная формула γ. Покажем, что ее оценка истинна тогда и только тогда, когда она входит в Γ (при условии, что это свойство выполнено для составных частей).

Конструкция здесь похожа на конструкцию при доказательстве полноты исчисления высказываний. Для примера рассмотрим конъюнкцию и отрицание:

- Пусть $[\![\alpha\&\beta]\!] = \text{И}$. Покажем, что $\alpha\&\beta \in \Gamma$.

  В самом деле, пусть это не так и $\neg(\alpha\&\beta) \in \Gamma$, а, значит, $\Gamma, \alpha\&\beta \vdash \psi\&\neg\psi$. Тогда $\Gamma, \alpha, \beta \vdash \psi\&\neg\psi$ (доказуемое утверждение $(\psi\&\phi \to \pi) \to (\psi \to \phi \to \pi)$ и теорема о дедукции).

  Из таблицы истинности конъюнкции следует, что она истинна только если обе ее составных части истинны. То есть $[\![\alpha]\!] = \text{И}$ и $[\![\beta]\!] = \text{И}$. Значит, $\alpha \in \Gamma$ и $\beta \in \Gamma$, что приводит к противоречивости Γ.

- Пусть $[\![\alpha\&\beta]\!] = \text{Л}$. Покажем, что $\neg(\alpha\&\beta) \in \Gamma$.

  Из таблицы истинности следует, что один из параметров обязательно ложен. Пусть, например, $[\![\alpha]\!] = \text{Л}$ (случай $[\![\beta]\!] = \text{Л}$ рассматривается аналогично). Тогда $\alpha \notin \Gamma$, и поэтому $\neg\alpha \in \Gamma$. Рассмотрим доказательство:

(1)	$\neg\alpha$	Предположение
(2)	$\neg\alpha \to \alpha\&\beta \to \neg\alpha$	Сх. акс. 1
(3)	$\alpha\&\beta \to \neg\alpha$	M.P. 1,2
(4)	$\alpha\&\beta \to \alpha$	Сх. акс. 4
(5)	$(\alpha\&\beta \to \alpha) \to (\alpha\&\beta \to \neg\alpha) \to \neg(\alpha\&\beta)$	Сх. акс. 9
(6)	$(\alpha\&\beta \to \neg\alpha) \to \neg(\alpha\&\beta)$	M.P. 5,4
(7)	$\neg(\alpha\&\beta)$	M.P. 6,3

  Значит, невозможно, чтобы $\alpha\&\beta \in \Gamma$, поскольку иначе получится, что Γ противоречиво.

- Пусть $[\![\neg\alpha]\!] = \text{И}$. Из оценки следует $[\![\alpha]\!] = \text{Л}$, то есть $\neg\alpha \in \Gamma$.

- Пусть $[\![\neg\alpha]\!] = \text{Л}$. Тогда $[\![\alpha]\!] = \text{И}$. То есть $\alpha \in \Gamma$. Значит, невозможно $\neg\alpha \in \Gamma$, иначе Γ было бы противоречиво.

□

7.3 Теорема Гёделя о полноте исчисления предикатов

Определение 7.4. Назовём формулу α формулой с поверхностными кванторами, если существует такой узел в дереве разбора формулы, не являющийся квантором, ниже которого нет ни одного квантора, а выше — нет ничего, кроме кванторов.

Например, формулы $\forall x\exists y\forall z(P(x,y,z)\&P(z,y,x))$ и $A\&B$ — это формулы с поверхностными кванторами, а формулы $A\&\forall xB(x)$, $\exists aP(a) \vee \exists bP(b)$ или $\neg\forall x(P(x) \to P(y))$ формулами с поверхностными кванторами не являются.

Лемма 7.6. Для любой формулы исчисления предикатов найдётся эквивалентная ей формула с поверхностными кванторами.

Доказательство. Доказательство индукцией по структуре формулы. Будем пошагово переносить кванторы на один уровень выше, при необходимости переименовывая переменные (если формула имеет вид $\exists x\alpha\&\exists x\beta$, мы ее в итоге преобразуем к виду $\exists x_1\exists x_2(\alpha[x := x_1]\&\beta[x := x_2])$ и раскрывая отрицания ($\neg\exists x\alpha$ превратится в $\forall x\neg\alpha$). □

Теорема 7.7. Теорема Гёделя о полноте исчисления предикатов. Пусть Γ — непротиворечивое множество формул исчисления предикатов. Тогда существует модель для Γ.

Доказательство. Без потери общности мы будем предполагать, что Γ содержит только формулы с поверхностными кванторами.

Для доказательства теоремы нам достаточно избавиться от кванторов, не потеряв непротиворечивости, и сослаться на 7.5. Для этого мы определим следующий процесс избавления от одного квантора. Мы построим новый язык, отличающийся от исходного дополнительными константами. Пусть эти новые константы имеют имена d_i^j (верхний индекс означает поколение — мы сперва добавим константы d_i^1, потом d_i^2 и т.п.).

Возьмем непротиворечивое множество формул Γ_g и пополним его дополнительными формулами, получив непротиворечивое множество Γ_{g+1}, такое что $\Gamma_g \subseteq \Gamma_{g+1}$.

Возьмем формулу $\gamma \in \Gamma_g$. Возможны такие варианты:

- γ не содержит кванторов. Оставим ее как есть.
- $\gamma \equiv \forall x\alpha$. Возьмем все константы, использующиеся в Γ_g (это будут c_i и только те d_i^j, которые добавлены раньше, т.е. $j \leq g$), и все выражения, которые мы можем из них построить с участием функциональных символов (их всё равно счётное количество), занумеруем их $(\theta_1, \theta_2, \dots)$ и добавим формулы $\alpha_1 \equiv \alpha[x := \theta_1], \alpha_2 \equiv \alpha[x := \theta_2], \dots$ к Γ_{g+1}.
- $\gamma \equiv \exists x\alpha$. Возьмем новую константу d_k^{g+1}, не использовавшуюся ранее, и добавим формулу $\alpha[x := d_k^{g+1}]$ к Γ_{g+1}.

Заметим, что все формулы с кванторами пока остаются в Γ_{g+1}, мы только добавляем бескванторные формулы. Такая схема позволяет сделать процесс управляемым (мы всегда добавляем новые переменные, что упрощает доказательства), но при этом корректным: ведь нам нужно добавлять по формуле $\forall x\alpha$ все возможные выражения $\alpha[x := \theta]$, не только с упоминаемыми в Γ_g константами. При данной схеме мы вернёмся неизбежно к новым (только что добавленным) константам при следующей итерации и добавим недостающие формулы.

Покажем, что так построенное множество формул останется непротиворечивым. Пусть это не так, и существует доказательство противоречия $\Gamma_{g+1} \vdash \beta\&\neg\beta$. Это доказательство использует конечное количество шагов, и, следовательно, мы можем явно выписать все его новые по сравнению с Γ посылки, перенеся их в правую часть по теореме о дедукции: $\Gamma_g \vdash \gamma_1 \to \dots \gamma_n \to \beta\&\neg\beta$.

Раз мы оставили справа только новые для Γ_g формулы, то каждая из формул γ_i была получена из какой-то исходной формулы из Γ_g путем удаления одного квантора. Мы будем, последовательно перебирая формулы и перестраивая доказательство, исключать формулы из правой части, пока не окажется, что предположив противоречивость Γ_{g+1}, мы получим противоречивость Γ_g.

Возможны два варианта:

- $\gamma_1 \equiv \alpha[x := \theta]$ получено из $\forall x\alpha$. Тогда рассмотрим доказательство:

(1)	$\forall x\alpha \to \alpha[x := \theta]$	Сх. акс. $\forall$
(2)	$\forall x\alpha$	$\forall x\alpha$ из Γ_g
(3)	$\alpha[x := \theta]$	M.P. $2, 1$
$(4 \dots k)$	$\alpha[x := \theta] \to (\gamma_2 \to \dots \gamma_n \to \beta\&\neg\beta)$	Исх. формула
$(k+1)$	$\gamma_2 \to \dots \gamma_n \to \beta\&\neg\beta$	M.P. $3, k$

- $\gamma_1 \equiv \alpha[x := d_k^{g+1}]$ получено из $\exists x\alpha$. Выберем какую-нибудь переменную, которая не участвует в выводе противоречия — пусть это y. Заменим все вхождения d_k^{g+1} в доказательстве на y. Поскольку d_k — константа, то никаких правил для кванторов мы не заденем, и доказательство останется верным. Заметим, что поскольку d_k^{g+1}

— константа, введенная специально для замены переменной x в данной формуле на шаге g и ранее не встречавшаяся — то она отсутствует в формулах $\gamma_2 \dots \gamma_n$. Также, мы можем правильно выбрать β, чтобы и в нем отсутствовала d_k^{g+1}. Значит, мы можем применить правило для введения $\exists$:

$(1 \dots k)$	$\alpha[x := y] \to (\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta)$	Исх. формула
$(k+1)$	$\exists y \alpha[x := y] \to (\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta)$	Правило для $\exists$
$(k+2)$	$\exists x \alpha$	Т.к. $\exists x \alpha$ из Γ_g
$(k+3 \dots l)$	$\exists y \alpha[x := y]$	Доказуемо
$(l+1)$	$\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta$	М.Р. $l, k+1$

Взяв $\Gamma_0 \equiv \Gamma$, получим последовательность $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \dots$. Положим $\Gamma^* \equiv \cup\Gamma_i$. Γ^* также не может быть противоречиво, поскольку доказательство использует конечное количество предположений, добавленных, максимум, на шаге g. Значит, множество Γ_g тоже противоречиво, что невозможно. Выделив в Γ^* бескванторное подмножество, пополнив его по теореме 7.2, по лемме 7.5 мы получаем модель для него.

Теперь покажем, что это модель и для всего Γ^* (а, значит, и для Γ).

Рассмотрим некоторую формулу $\gamma \in \Gamma^*$, покажем, что $[\![\gamma]\!] = \text{И}$. Проверку мы будем вести индукцией по структуре «кванторного» префикса формулы.

База. Формула не содержит кванторов. В этом случае истинность гарантирует лемма 7.5.

Переход. Пусть это модель для любой формулы из Γ^* с r кванторами. Покажем, что она остаётся моделью и для формул из Γ^* с $r+1$ квантором. Пусть формула γ впервые добавлена на шаге p к Γ_p. Тогда рассмотрим случаи:

- $\gamma \equiv \forall x \psi$. Нам нужно показать, что формула истинна при любом $t \in D$. Возьмём некоторый t. По построению модели, есть такое θ — выражение из констант и функциональных символов, что $\text{«}\theta\text{»} \equiv t$.

  По построению же Γ^*, начиная с шага $p+1$ мы будем добавлять все формулы вида $\psi[x := \kappa]$, где κ — некоторая конструкция из констант и функциональных символов.

  Также, каждая из констант c_i или d_i^j из θ добавлена на некотором шаге s_k. То есть, как только и константы и формула окажутся в Γ_l (понятно, что $l = max(max(s_k), p)$), так сразу, начиная с Γ_{l+1} в нём будет присутствовать и $\psi[x := \theta]$. В формуле ψ на один квантор меньше — и, по предположению индукции, поэтому она истинна.

- $\gamma \equiv \exists x \psi$. Аналогично, по построению Γ^*, как только ψ добавляется к Γ_g, так сразу формула $\psi[x := d_k^{g+1}]$ появляется в Γ_{g+1}. Значит, ψ истинна на значении $\text{«}d_k^{g+1}\text{»}$, то есть γ истинна.

□

Теорема 7.8. Если $\models \alpha$, то $\vdash \alpha$.

Доказательство. Рассмотрим множество $\Gamma \equiv \{\neg\alpha\}$. Если α недоказуемо, то Γ непротиворечиво, и у Γ есть модель, причём $\Gamma \models \neg\alpha$. Значит, неверно, что $\models \alpha$. □

8 Теории первого порядка

Мы занимались до этого момента только логическими рассуждениями самими по себе. Это интересно, но не очень практически полезно: мы все-таки используем логические рассуждения для доказательства утверждений о каких-то объектах. Было бы разумно каким-то образом включить эти объекты в рамки формальной теории.

Рассмотрим некоторое множество N. Будем говорить, что оно удовлетворяет аксиомам Пеано, если выполнено следующее:

- В нем существует некоторый выделенный элемент 0.
- Для каждого элемента множества определена операция $'$.

Кроме того, эти элемент и операция должны удовлетворять следующим требованиям:

- Не существует такого x, что $x' = 0$.
- Если $x' = y'$, то $x = y$.
- Если некоторое предположение верно для 0, и если из допущения его для n можно вывести его истинность для $n + 1$, то предположение верно для любого элемента множества.

Данная аксиоматика позволяет определить натуральные числа (множество натуральных чисел — это множество, удовлетворяющее аксиомам Пеано; заметим, что тут натуральные числа содержат 0, так оказывается удобнее) и операции над ними. Например, сложение можно задать следующими уравнениями:

$$a + 0 = a$$
$$a + b' = (a + b)'$$

Теорема 8.1. Так определенное сложение коммутативно.

Доказательство. Упражнение. □

Но данная аксиоматика сформулирована неформально, поэтому мы не сможем доказать никаких содержательных утверждений про нее, пользуясь формальными средствами. Поэтому нам нужно эту конструкцию как-то объединить с исчислением предикатов, чем мы сейчас и займемся.

Возьмем язык исчисления предикатов со следующими изменениями и особенностями:

- Маленькими латинскими буквами a,b,... (возможно, с индексами) будем обозначать индивидные переменные.
- К логическим связкам добавляются такие: $(=)$ — двуместный предикат, $(+)$ и $(\cdot)$ — двуместные функции, и $(')$ — одноместная функция. Все левоассоциативное, приоритеты в порядке убывания: $(')$, потом $(\cdot)$, потом $(+)$. Все логические связки имеют приоритет ниже. Например, $a = b' + b' + c \cdot c \& b = c$ надо интерпретировать как $(a = (((b') + (b')) + (c \cdot c))) \& (b = c)$.
- Вводится 0-местная функция 0.

К стандартным аксиомам исчисления предикатов добавим следующие 8 *нелогических* аксиом и одну нелогическую схему аксиом.

(A1) $a = b \to a' = b'$
(A2) $a = b \to a = c \to b = c$
(A3) $a' = b' \to a = b$
(A4) $\neg a' = 0$
(A5) $a + b' = (a + b)'$
(A6) $a + 0 = a$
(A7) $a \cdot 0 = 0$
(A8) $a \cdot b' = a \cdot b + a$
(A9) $(\psi[x := 0])\&\forall x((\psi) \to (\psi)[x := x']) \to (\psi)$

В схеме аксиом (A9) ψ – некоторая формула исчисления предикатов и x — некоторая переменная, входящая свободно в ψ.

Теорема 8.2. $\vdash a = a$

Доказательство. Упражнение. Клини, стр. 254. □

Определение 8.1. Структура. Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P\rangle$, где $F = \langle F_0, F_1, ...\rangle$ — списки оценок для 0-местных, 1-местных и т.д. функций, и $P = \langle P_0, P_1, ...\rangle$ — списки оценок для 0-местных, 1-местных и т.д. предикатов, D — предметное множество.

Понятие структуры — развитие понятия оценки из исчисления предикатов. Но оно касается только нелогических составляющих теории; истинностные значения и оценки для связок по-прежнему определяются исчислением предикатов, лежащим в основе теории. Для получения оценки формулы нам нужно задать структуру, значения всех свободных индивидных переменных, и (естественным образом) вычислить результат.

Определение 8.2. Назовем структуру корректной, если любая доказуемая формула истинна в данной структуре.

Определение 8.3. Моделью теории мы назовем любую корректную структуру.

Еще одним примером теории первого порядка может являться теория групп. К исчислению предикатов добавим двуместный предикат $(=)$, двуместную функцию $(\cdot)$, одноместную функцию (x^{-1}), константу (т.е. 0-местную функцию) 1 и следующие аксиомы:

(E1) $a = b \to (a = c \to b = c)$
(E2) $a = b \to (a \cdot c = b \cdot c)$
(E3) $a = b \to (c \cdot a = c \cdot b)$
(G1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(G2) $a \cdot 1 = a$
(G3) $a \cdot a^{-1} = 1$

Теорема 8.3. Доказуемо, что $a = b \to b = a$ и что $a^{-1} \cdot a = 1$.

Доказательство. Упражнение. □

9 Рекурсивные функции.

Рассмотрим примитивы, из которых будем собирать выражения:

1. $Z : N \to N$, $Z(x) = 0$
2. $N : N \to N$, $N(x) = x'$
3. Проекция. $U_i^n : N^n \to N$, $U_i^n(x_1, ...x_n) = x_i$
4. Подстановка. Если $f : N^n \to N$ и $g_1, ...g_n : N^m \to N$, то $S\langle f, g_1, ...g_n\rangle : N^m \to N$. При этом $S\langle f, g_1, ...g_n\rangle(x_1, ...x_m) = f(g_1(x_1, ...x_m), ...g_n(x_1, ...x_m))$
5. Примитивная рекурсия. Если $f : N^n \to N$ и $g : N^{n+2} \to N$, то $R\langle f, g\rangle : N^{n+1} \to N$, при этом
$$R\langle f, g\rangle(x_1, ...x_n, y) = \begin{cases} f(x_1, ...x_n) & , y = 0 \\ g(x_1, ...x_n, y-1, R\langle f, g\rangle(x_1, ...x_n, y-1)) & , y > 0 \end{cases}$$
6. Минимизация. Если $f : N^{n+1} \to N$, то $\mu\langle f\rangle : N^n \to N$, при этом $\mu\langle f\rangle(x_1, ...x_n)$ — такое минимальное число y, что $f(x_1, ...x_n, y) = 0$. Если такого y нет, результат данного примитива неопределен.

Если некоторая функция $N^n \to N$ может быть задана с помощью данных примитивов, то она называется рекурсивной. Если некоторую функцию можно собрать исключительно из первых 5 примитивов (то есть без использования операции минимизации), то такая функция называется примитивно-рекурсивной.

Теорема 9.1. Следующие функции являются примитивно-рекурсивными: сложение, умножение, ограниченное вычитание (которое равно 0, если результат вычитания отрицателен), целочисленное деление, остаток от деления, проверка значения на простоту.

Доказательство. Упражнение. □

Интересен вопрос — если столь сложные функции, как вычисление простых чисел, являются примитивно-рекурсивными, то не достаточно ли их будет для вычисления любой функции? А если нет, то каков пример функции, не являющейся примитивно-рекурсивной.

Классическим примером рекурсивной, но не примитивно-рекурсивной, функции является функция Аккермана.

Определение 9.1. Функцией *Аккермана* мы назовем так определенную функцию:

$$A(m, n) = \begin{cases} n+1, & \text{если } m = 0 \\ A(m-1, n), & \text{если } m > 0, n = 0 \\ A(m-1, A(m, n-1)), & \text{если } m > 0, n > 0 \end{cases}$$

Также нам будет удобно другое обозначение: $\alpha_m(n) = A(m, n)$. Данное обозначение позволяет рассматривать функцию Аккермана как семейство функций от одной переменной.

Лемма 9.2. $\alpha_{m+1}(n) = \alpha_m^{n+1}(1)$.

Доказательство. Докажем индукцией по n.

База индукции: $\alpha_m(0) = A(m, 0) = A(m-1, 1) = \alpha_{m-1}^{0+1}(1)$.

Переход: пусть $\alpha_{m+1}(n) = \alpha_m^{n+1}(1)$. Тогда $\alpha_{m+1}(n+1) = A(m+1, n+1) = A(m, A(m+1, n)) = \alpha_m(\alpha_m^{n+1}(1)) = \alpha_m^{n+2}(1)$ □

Лемма 9.3. Для функции Аккермана справедливы следующие свойства:

1. Если $m_1 < m_2$, то $A(m_1, n) < A(m_2, n)$
2. Если $n_1 < n_2$, то $A(m, n_1) < A(m, n_2)$
3. $\alpha_1(n) = n + 2$
4. $\alpha_2(n) = 2n + 3$
5. $\alpha_{m+2}(n) > \alpha_m^{n+2}(n)$

Доказательство. Первые четыре свойства достаточно легко показать по индукции. Покажем последнее.

Согласно определению функции Аккермана, и предыдущим пунктам леммы, справедлива цепочка равенств и неравенств: $\alpha_{m+2}(n) = \alpha_{m+1}^{n+1}(1) = \alpha_{m+1}(\alpha_{m+1}^n(1)) = \alpha_m^{\alpha_{m+1}^n(1)+1}(1) = \alpha_m^{\alpha_{m+2}(n-1)+1}(1) \geq \alpha_m^{\alpha_2(n-1)+1}(1) = \alpha_m^{2(n-1)+3+1}(1) = \alpha_m^{n+n+2}(1) = \alpha_m^{n+2}(\alpha_m^n(1))$ Поскольку $\alpha_m^n(1) \geq \alpha_0^n(1) = inc^n(1) = n + 1$, то $\alpha_m^n(1) > n$, то есть $\alpha_m^{n+2}(\alpha_m^n(1)) > \alpha_m^{n+2}(n)$.

□

Введем обозначение: если задан некоторый набор значений $x_1, \ldots x_n$, то для упрощения записи будем писать $\overrightarrow{x}$ вместо него. Например, если задана некоторая функция $f : N^n \to N$, то будем писать $f(\overrightarrow{x})$ вместо $f(x_1, \ldots, x_n)$. Запись же $g(\overrightarrow{x}, y)$ означает, что функция g применяется к $n + 1$ аргументу: $g(x_1, \ldots, x_n, y)$.

Теорема 9.4. Функция Аккермана растет быстрее любой примитивно-рекурсивной функции. Точнее, какова бы ни была примитивно-рекурсивная фукнция $p : N^n \to N$, мы можем подобрать такую константу K, что $p(\overrightarrow{x}) \leq \alpha_K(\max(\overrightarrow{x}))$ при любом x.

Доказательство. Докажем индукцией по структуре формулы, показывающей примитивную рекурсивность p. Базой будут являться примитивы Z,N и U, для которых утверждение очевидно. Покажем переход для примитивов S и R.

Рассмотрим примитив S. Пусть $p = S\langle f, g_1, \ldots g_m\rangle$, где $f, g_1, \ldots g_m$ — это некоторые примитивно-рекурсивные функции, для которых по предположению индукции уже найдены требуемые константы $K_0, K_1 \ldots K_m$. Тогда возьмем $K = max(K_0 \ldots K_m)+2$, и покажем, что это значение нас устроит. В самом деле:

$$p(\overrightarrow{x}) = f(g_1(\overrightarrow{x}), \ldots g_m(\overrightarrow{x})) \leq \alpha_{K_0}(max(g_1(\overrightarrow{x}), \ldots g_m(\overrightarrow{x})) \leq \alpha_{K-2}(max(g_1(\overrightarrow{x}), \ldots g_m(\overrightarrow{x}))$$

В свою очередь, каждый g_i мы можем оценить через соответствующий α_{K_i}:

$$g_i(\overrightarrow{x}) \leq \alpha_{K_i}(max(\overrightarrow{x})) \leq \alpha_{K-2}(max(\overrightarrow{x}))$$

из чего получается, что

$$\alpha_{K-2}(max(g_1(\overrightarrow{x}), \ldots g_m(\overrightarrow{x}))) \leq \alpha_{K-2}(\alpha_{K-2}(max(\overrightarrow{x}))) \leq \alpha_{K-2}^{max(\overrightarrow{x})+2}(max(\overrightarrow{x}))$$

Применив свойство из предыдущей леммы, мы можем заключить требуемое:

$$\alpha_{K-2}^{max(\overrightarrow{x})+2}(max(\overrightarrow{x})) < \alpha_K(max(\overrightarrow{x}))$$

Теперь рассмотрим примитив R: $p = R\langle g, h\rangle$, причём $f : N^{n-1} \to N$, и $g : N^{n+1} \to N$, и для них уже найдены константы K_1 и K_2, соответственно. Тогда возьмем $K = max(K_1, K_2) + 2$.

Для доказательства утверждения покажем чуть более сильное утверждение:

$$p(\overrightarrow{x}, y) \leq \alpha_{K-2}^{y+1}(max(\overrightarrow{x}, y))$$

Этого достаточно, поскольку

$$\alpha_{K-2}^{y+1}(max(\overrightarrow{x}, y)) \leq \alpha_{K-2}^{max(\overrightarrow{x},y)+1}(max(\overrightarrow{x}, y)) \leq$$

$$\leq \alpha_{K-2}^{max(\overrightarrow{x},y)+2}(max(\overrightarrow{x}, y)) < \alpha_K(max(\overrightarrow{x}, y))$$

Покажем требуемое индукцией по y. База: $y = 0$. Тогда:

$$p(\overrightarrow{x}, 0) = f(\overrightarrow{x}) \leq \alpha_{K_1}(max(\overrightarrow{x}) = \alpha_{K_1}(max(\overrightarrow{x}, 0)) \leq \alpha_{K-2}(max(\overrightarrow{x}, 0))$$

Переход: пусть $p(\overrightarrow{x}, y) \leq \alpha_{K-2}^{y+1}(max(\overrightarrow{x}, y))$. Тогда

$$p(\overrightarrow{x}, y+1) = g(\overrightarrow{x}, y, p(\overrightarrow{x}, y)) \leq \alpha_{K_2}(max(\overrightarrow{x}, y, p(\overrightarrow{x}, y))) \leq$$

$$\leq \alpha_{K_2}(max(\overrightarrow{x}, y, \alpha_{K-2}^{y+1}(max(\overrightarrow{x}, y))) =$$

(тут используется монотонность α)

$$= \alpha_{K_2}(\alpha_{K-2}^{y+1}(max(\overrightarrow{x}, y))) \leq \alpha_{K-2}^{y+2}(max(\overrightarrow{x}, y+1))$$

□

Теорема 9.5. Функция Аккермана не является примитивно-рекурсивной.

Доказательство. Пусть это не так, и функция $A(x, y)$ — примитивно-рекурсивна. Тогда рассмотрим $g(x) = A(x, x)$. Эта функция, очевидно, тоже является примитивно-рекурсивной.

Однако, по предыдущей теореме, найдется такой N, что $g(x) \leq A(N, x)$ при любом x. В том числе это верно и при $x = N+1$. То есть, по предыдущей теореме, $g(N+1) = A(N+1, N+1) \leq A(N, N+1)$, однако нам также известно, что $A(N+1, N+1) > A(N, N+1)$. □

10 Арифметические функции и отношения. Их выразимость в формальной арифметике.

Введем обозначение. Если в тексте вводится некоторая формула $\alpha(x_1, \ldots x_n)$, то по умолчанию считается, что эта формула имеет минимум n свободных переменных, с именами $x_1, \ldots x_n$

Внутри же выражения запись $\alpha(y_1, \ldots y_n)$ мы будем трактовать, как $\alpha[x_1 := y_1, ...x_n := y_n]$, при этом мы подразумеваем, что $y_1, \ldots y_n$ свободны для подстановки вместо $x_1, \ldots x_n$ в α.

Также, запись $B(x_1, \ldots x_n) \equiv \alpha(x_1, \ldots x_n)$ будет означать, что мы определяем новую формулу с именем B и n свободными переменными $x_1, \ldots x_n$. Данная формула должна восприниматься только как сокращение записи, макроподстановка.

Определение 10.1. Арифметическая функция — функция $f : N^n \to N$. Арифметическое отношение — n-арное отношение, заданное на N.

Определение 10.2. Арифметическое отношение R называется выразимым (в формальной арифметике), если существует такая формула $\alpha(x_1, \ldots x_n)$ с n свободными переменными, что для любых натуральных чисел k_1 ... k_n

1. если $(k_1, \dots k_n) \in R$, то доказуемо $\alpha(\overline{k_1}, \dots \overline{k_n})$

2. если $(k_1, \dots k_n) \notin R$, то доказуемо $\neg\alpha(\overline{k_1}, \dots \overline{k_n})$.

Например, отношение $(<)$ является выразимым в арифметике: Рассмотрим формулу $\alpha(a_1, a_2) = \exists b(\neg b = 0 \& a_1 + b = a_2)$. В самом деле, если взять некоторые числа k_1 и k_2, такие, что $k_1 < k_2$, то найдется такое положительное число b, что $k_1 + b = k_2$. Можно показать, что если подставить $\overline{k_1}$ и $\overline{k_2}$ в α, то формула будет доказуема.

Наметим доказательство: Тут должно быть два доказательства по индукции, сперва по k_2, потом по k_1. Рассмотрим доказательство по индукции: пусть $k_1 = 0$, индукция по 2-му параметру: Разберем доказательство базы при $k_2 = 1$. Тогда надо показать $\exists b(\neg b = 0 \& 0 + b = 1)$:

(1)	$\neg 1 = 0 \& 0 + 1 = 1$	Несложно показать
(2)	$(\neg 1 = 0 \& 0 + 1 = 1) \to \exists b(\neg b = 0 \& 0 + b = 1)$	Сх. акс. для $\exists$
(3)	$\exists b(\neg b = 0 \& 0 + b = 1)$	М.Р. 1 и 2.

Определение 10.3. Введем следующее сокращение записи: пусть $\exists! y\phi(y)$ означает

$$\exists y\phi(y) \& \forall a \forall b(\phi(a) \& \phi(b) \to a = b)$$

Здесь a и b — некоторые переменные, не входящие в формулу ϕ свободно.

Определение 10.4. Арифметическая функция f от n аргументов называется представимой в формальной арифметике, если существует такая формула $\alpha(x_1, \dots x_{n+1})$ с $n+1$ свободными пременными, что для любых натуральных чисел k_1 ... k_{n+1}

1. $f(k_1, \dots k_n) = k_{n+1}$ тогда и только тогда, когда доказуемо $\alpha(\overline{k_1}, \dots \overline{k_{n+1}})$.

2. Доказуемо $\exists! b(\alpha(\overline{k_1}, \dots \overline{k_n}, b)$

Теорема 10.1. Функции Z, N, U_i^n являются представимыми.

Доказательство. Наметим доказательство. Для этого приведем формулы, доказательство корректности этих формул оставим в виде упражнения.

- Примитив Z представит формула $Z(a, b) := (a = a \& b = 0)$.
- Примитив N представит формула $N(a, b) := (a' = b)$.
- Примитив U_i^n представит формула $U_i^n(a_1, ...a_n, b) = (a_1 = a_1) \& ... \& (a_n = a_n) \& (b = a_i)$.

□

Теорема 10.2. Если функции f и g_1, ... g_m представимы, то функция $S\langle f, g_1, \dots g_m\rangle$ также представима.

Доказательство. Поскольку функции f и g_i представимы, то есть формулы F и $G_1, \dots G_m$, их представляющие. Тогда следующая формула представит $S\langle f, g_1, \dots g_m\rangle$:

$$S(a_1, \dots a_n, b) := \exists b_1 \dots \exists b_m(G_1(a_1, \dots a_n, b_1) \& \dots \& G_m(a_1, \dots a_n, b_m) \& F(b_1, \dots b_m, b))$$

□

Определение 10.5. β-функция Геделя - это функция $\beta(b, c, i) = b\%(1 + c \cdot (i + 1))$. Здесь операция $(\%)$ означает взятие остатка от целочисленного деления.

Лемма 10.3. Функция примитивно-рекурсивна, и при этом представима в арифметике формулой $B(b,c,i,d) := \exists q((b = q \cdot (1 + c \cdot (i+1)) + d) \& (d < 1 + c \cdot (i+1)))$

Доказательство. Упражнение. □

Теорема 10.4. Китайская теорема об остатках. Если $u_1, \dots u_n$ — попарно взаимно простые целые числа, и $k_1, \dots k_n$ — целые числа, такие, что $0 \le k_i < u_i$ при любом i, то найдется такое целое число b, что $k_i = b\%u_i$ при любом i.

Доказательство этой теоремы по индукции несложно, но не входит в наш курс.

Лемма 10.5. Для любой конечной последовательности чисел k_0 ... k_n можно подобрать такие константы b и c, что $\beta(b,c,i) = k_i$ для $0 \le i \le n$.

Доказательство. Возьмем число $c = max(k_1, \dots k_n, n)!$. Рассмотрим числа $u_i = 1 + c \cdot (i+1)$.

- Никакие числа u_i и u_j $(0 \le j < i \le n)$ не имеют общих делителей кроме 1. Пусть это не так, и есть некоторый общий делитель p (очевидно, мы можем предположить его простоту — разложив на множители, если он составной). Тогда p будет делить $u_i - u_j = c \cdot (i-j)$, при этом p не может делить c — иначе окажется, что $u_i = (1 + c \cdot (i+1))$ делится на p и $c \cdot (i+1)$ делится на p. Значит, p делит $i - j$, то есть все равно делит c, так как c — факториал некоторого числа, не меньшего n, и при этом $i - j \le n$.
- Каждое из чисел k_i меньше, чем u_i: в самом деле, $k_i \le c < 1 + c \cdot (i+1) = u_i$.

  Из полученных утверждений видно, что выполнены условия китайской теоремы об остатках. Следовательно, найдется такое целое число b, для которого выполнено $k_i = b\%u_i$, то есть $k_i = \beta(b,c,i)$.

□

Теорема 10.6. Всякая рекурсивная функция представима в арифметике.

Доказательство. Представимость первых четырех примитивов уже показана. Покажем представимость примитивной рекурсии и операции минимизации.

Примитивная рекурсия. Пусть есть некоторый $R\langle f, g\rangle$. Соответственно, f и g уже представлены как некоторые формулы F и G. Из определения $R\langle f, g\rangle$ мы знаем, что для значения $R\langle f, g\rangle(x_1, ...x_{n+1})$ должна существовать последовательность $a_0 ... a_{x_{n+1}}$ результатов применения функций f и g — значений на одно больше, чем итераций в цикле примитивной рекурсии, а это количество определяется последним параметром функции $R\langle f, g\rangle$. При этом:

$a_0 = f(x_1, \dots x_n)$
$a_1 = g(x_1, \dots x_n, 0, a_0)$
...
$a_{x_{n+1}} = g(x_1, \dots x_n, x_{n+1} - 1, a_{x_{n+1}-1})$

Значит, по лемме, должны существовать такие числа b и c, что $\beta(b,c,i) = a_i$ для $0 \le i \le x_{n+1}$.

Приведенные рассуждения позволяют построить следующую формулу, представляющую $R\langle f, g\rangle(x_1, ...x_{n+1})$:

$$R(x_1, \dots x_{n+1}, a) := \exists b \exists c(\exists k(B(b,c,0,k) \& F(x_1, ...x_n, k)) \\ \& B(b,c,x_{n+1},a) \\ \& \forall k(k < x_{n+1} \to \exists d \exists e(B(b,c,k,d) \& B(b,c,k',e) \& G(x_1, ..x_n, k, d, e)))$$

Минимизация. Рассмотрим конструкцию $\mu\langle f\rangle$. f уже представлено как некоторая формула F. Тогда формула $M(x_1, \dots x_n, y) := F(x_1, \dots x_n, y, 0) \& \forall z(z < y \to \neg F(x_1, \dots x_n, z, 0))$ представит $\mu\langle f\rangle$.

□

11 Гёделева нумерация. Арифметизация доказательств

Ранее мы показали, что любое рекурсивное арифметическое отношение выразимо в формальной арифметике. Теперь мы покажем, что любое выразимое в формальной арифметике отношение является рекурсивным.

Определение 11.1. Ограниченные кванторы $\exists_{x<y}\phi(x)$ и $\forall_{x<y}\phi(x)$ — сокращения записи для выражений вида $\exists x(x < y \& \phi(x))$ и $\forall x(x \geq y \vee \phi(x))$

Теорема 11.1. Пусть P_1 и P_2 — рекурсивные отношения. Тогда следующие формулы, задающие некоторые отношения, также являются рекурсивными отношениями:

1. $F(x_1, \dots x_n, z) := \forall_{y<z} P_1(x_1, \dots x_n, y)$
2. $E(x_1, \dots x_n, z) := \exists_{y<z} P_1(x_1, \dots x_n, y)$
3. $P_1(x_1, \dots x_n) \to P_2(x_1, \dots x_n)$
4. $P_1(x_1, \dots x_n) \vee P_2(x_1, \dots x_n)$
5. $P_1(x_1, \dots x_n) \& P_2(x_1, \dots x_n)$
6. $\neg P_1(x_1, \dots x_n)$

Доказательство. Упражнение. □

Теперь мы перенесем понятие вывода формулы на язык рекурсивных отношений, и, следовательно, внутрь языка формальной арифметики.

Определение 11.2. Гёделева нумерация.Дадим следующие номера символам языка формальной арифметики:

3	(	
5	)	
7	,	
9	$\neg$	
11	$\to$	
13	$\vee$	
15	&	
17	$\forall$	
19	$\exists$	
$21 + 6 \cdot k$	x_k	переменные
$23 + 6 \cdot 2^k \cdot 3^n$	f_k^n	n-местные функциональные символы: $(')$, $(+)$ и т.п.
$25 + 6 \cdot 2^k \cdot 3^n$	P_k^n	n-местные предикаты, в т.ч. $(=)$

Уточним язык — обяжем всегда писать скобки всегда и только вокруг двуместной операции. В принципе, иначе мы могли бы определить правильно операцию равенства Eq, но это лишние технические сложности. Также укажем номера для предопределенных функций и предикатов: $f_0^1 \equiv (')$, $f_0^2 \equiv (+)$, $f_1^2 \equiv (\cdot)$, $P_0^2 \equiv (=)$.

Научимся записывать выражения в виде чисел. Пусть $p_1, \dots p_k, \dots$ — список простых чисел, при этом $p_1 = 2, p_2 = 3, \dots$.

Тогда текст из n символов с гёделевыми номерами $c_1, \dots c_n$ запишем как число $t = p_1^{c_1} \cdot p_2^{c_2} \cdot \dots \cdot p_n^{c_n}$. Ясно, что такое представление однозначно позволяет установить длину строки (гёделева нумерация не содержит 0, поэтому можно определить длину строки как

максимальный номер простого числа, на которое делится t; будем записывать эту функцию как $Len(s)$), и каждый символ строки в отдельности (будем записывать функцию как $(s)_n$). Также ясно, что функции Len и $(x)_n$ — рекурсивны.

Чтобы удобнее работать со строками, введем следующие обозначения, за которыми скрываются рекурсивные функции:

- запись «$c_1c_2c_3\ldots$» (где c_i — какие-то символы языка формальной арифметики) задает рекурсивную функцию $f : N \to N$, при этом $f(x) = p_1^{c_1} \cdot \cdots \cdot p_n^{c_n}$.
- Операцию конкатенации строк определим так. Пусть S и T — рекурсивные функции, результат вычисления которых являются числа $s = p_1^{s_1} \cdot \cdots \cdot p_n^{s_n}$ и $t = p_1^{t_1} \cdot \cdots \cdot p_m^{s_m}$ соответственно. Тогда $S@T$ — это рекурсивная функция, вычисляющая функции S и T, результатом работы которой будет $p_1^{s_1} \cdot \cdots \cdot p_n^{s_n} \cdot p_{n+1}^{t_1} \cdot \cdots \cdot p_{n+m}^{t_m}$.

Чтобы представить доказательства, мы будем объединять строки вместе так же, как объединяем символы в строки: $2^{2^3} \cdot 3^{2^5}$ — это последовательность из двух строк, первая — это «(», а вторая — «)».

Теперь мы можем понять, как написать программу, проверяющую корректность доказательства некоторого утверждения в формальной арифметике. Наметим общую идею. Программа будет состоять из набора рекурсивных отношений и функций, каждое из которых выражает некоторое отношение, содержательное для проверки доказательства. Ниже мы покажем идею данной конструкции, приведя несколько из них.

- Проверка того, что a - строка, состоящая только из переменной. $Var(a) \equiv \exists_{z<a}(a = 2^{21+6\cdot z})$
- Проверка того, что выражение с номером a получено из выражений b и c путем применения правила Modus Ponens. $MP(b, c, a) \equiv c =$ «(» @ b @ « → » @ a @ «)»
- Проверка того, что b получается из a подстановкой y вместо x: $Subst(a, b, x, y)$ — без реализации
- Функция, подставляющая y вместо x в формуле a:
  $Sub(a, x, y) \equiv \mu\langle S\langle Subst, U_1^4, U_4^4, U_2^4, U_3^4\rangle\rangle(a, x, y)$
- Проверка того, что переменная номер x входит свободно в формулу f.
  $Free(f, x) \equiv \neg Subst(a, a, x, 21 + 6x)$
- Функция, выдающая гёделев номер выражения, соответствующего целому числу:
  $Num \equiv S\langle R\langle$«0»$, S\langle$@$, U_3^3, S\langle$«′»$, U_1^3\rangle\rangle\rangle, U_1^1, U_1^1\rangle$

Путем некоторых усилий мы можем выписать формулу, представляющую двуместное отношение $Proof(f, p)$, истинное тогда и только тогда, когда p — гёделев номер доказательства формулы с гёделевым номером f.

Теорема 11.2. Любая представимая в формальной арифметике функция является рекурсивной.

Доказательство. Возьмем некоторую представимую функцию $f : N^n \to N$. Значит, для нее существует формула формальной арифметики, представляющая ее. Пусть ϕ — эта формула (со свободными переменными $x_1, \ldots x_n, y$); при этом в случае $f(u_1, \ldots u_n) = v$ должно быть доказуемо $\phi(\overline{u_1}, \ldots \overline{u_n}, \overline{v})$. По формуле можно построить рекурсивную функцию, $C_\phi(u_1, \ldots u_n, v, p)$, выражающую тот факт, что p — гёделев номер вывода формулы $\phi(\overline{u_1}, \ldots \overline{u_n}, \overline{v})$. Тогда возьмем

$$f(x_1, \ldots x_n) \equiv (\mu\langle S\langle C_\phi, U_1^{n+1}, \ldots U_n^{n+1}, (U_{n+1}^{n+1})_1, (U_{n+1}^{n+1})_2\rangle\rangle(x_1, \ldots x_n))_1$$

. □

12 1я и 2я теоремы Геделя о неполноте арифметики

Определение 12.1. Мы будем называть теорию непротиворечивой, если не найдется такой формулы α, что доказуемо как α, так и $\neg\alpha$.

Лемма 12.1. Если теория противоречива, то в ней доказуема любая формула.

Доказательство. Если теория противоречива, то в ней есть утверждение α, что доказуемо α и $\neg\alpha$. Воспользуемся общезначимой (и потому доказуемой) формулой исчисления высказываний $\alpha \to \neg\alpha \to \beta$. □

Определение 12.2. Мы будем называть теорию ω-непротиворечивой, если, какова бы ни была формула $P(x)$ со свободной переменной x, такая, что для любого натурального числа p доказуемо $P(\overline{p})$, то формула $\exists p \neg P(p)$ недоказуема.

Лемма 12.2. ω-непротиворечивость влечёт непротиворечивость.

Доказательство. Рассмотрим выводимую формулу $x = x \to x = x$. При подстановке любого натурального числа вместо x формула будет по-прежнему выводима: $\overline{k} = \overline{k} \to \overline{k} = \overline{k}$. Значит, по ω-непротиворечивости формула $\exists p \neg (x = x \to x = x)$ невыводима. Значит, теория непротиворечива (поскольку в противоречивой теории выводится любая формула). □

Определим рекурсивное отношение $W_1(x, p)$, истинное тогда и только тогда, когда x есть гёделев номер формулы ϕ с единственным свободным аргументом x, а p есть гёделев номер доказательства $\phi(\text{«}\phi\text{»})$ — доказательства самоприменения ϕ. Это соотношение является выразимым в формальной арифметике с помощью следующей формулы:

$$\omega_1(x, p) \equiv Free(x, \text{«}x\text{»}) \& Proof(Sub(x, \text{«}x\text{»}, Num(x)), p)$$

Рассмотрим формулу $\sigma \equiv \forall p \neg \omega_1(x, p)$ — это некоторая формула с единственной свободной переменной x — и посмотрим, что произойдёт с её самоприменением: $\sigma(\overline{\text{«}\sigma\text{»}})$. Внимательное наблюдение за происходящим даст следующую теорему.

Теорема 12.3. Первая теорема Гёделя о неполноте арифметики.

1. Если формальная арифметика непротиворечива, то недоказуемо $\sigma(\overline{\text{«}\sigma\text{»}})$.
2. Если формальная арифметика ω-непротиворечива, то недоказуемо $\neg\sigma(\overline{\text{«}\sigma\text{»}})$.

Доказательство. 1. Пусть $\vdash \sigma(\overline{\text{«}\sigma\text{»}})$. Тогда найдется гёделев номер ее доказательства p, значит, $W_1(\text{«}\sigma\text{»}, p)$, то есть $\vdash \omega_1(\overline{\text{«}\sigma\text{»}}, \overline{p})$. С другой стороны, пользуясь схемой аксиом для квантора всеобщности и правилом Modus Ponens, из предположения теоремы $\vdash \sigma(\overline{\text{«}\sigma\text{»}})$ (то есть $\vdash \forall p \neg \omega_1(\overline{\text{«}\sigma\text{»}}, p)$) можно показать $\vdash \neg\omega_1(\overline{\text{«}\sigma\text{»}}, \overline{p})$. Противоречие.

2. Пусть $\vdash \neg\sigma(\overline{\text{«}\sigma\text{»}})$, то есть $\vdash \neg\forall p \neg\omega_1(\overline{\text{«}\sigma\text{»}}, p)$, то есть $\vdash \exists p \omega_1(\overline{\text{«}\sigma\text{»}}, p)$. Значит, неизбежно найдется такой номер q, что $\vdash \omega_1(\overline{\text{«}\sigma\text{»}}, \overline{q})$, поскольку если бы для каждого q было бы доказуемо $\vdash \neg\omega_1(\overline{\text{«}\sigma\text{»}}, \overline{q})$, то по ω-непротиворечивости было бы недоказуемо $\exists p \neg\neg\omega_1(\overline{\text{«}\sigma\text{»}}, p)$.

Рассмотрев же определение W_1, можно заметить, что найденный q также есть номер доказательства $\sigma(\overline{\text{«}\sigma\text{»}})$, что вступает в противоречие с предположением $\vdash \neg\sigma(\overline{\text{«}\sigma\text{»}})$. □

Формула $\sigma(\overline{\text{«}\sigma\text{»}})$, говоря простым языком, утверждает собственную недоказуемость. Мы показали, что эта формула (при условии ω-непротиворечивости формальной арифметики) действительно недоказуема — что означает её общезначимость. Таким образом, мы показали, что если формальная арифметика ω-непротиворечива, то она неполна.

В данном рассуждении используется сложное понятие ω-непротиворечивости, что смущает. Теорема Гёделя в форме Россера снимает эту сложность.

Рассмотрим отношение $W_2(x,p)$ — x и p состоят в отношении W_2 тогда и только тогда, когда p - гёделев номер доказательства *отрицания* самоприменения x (если ϕ — формула от одной переменной x, то p — номер доказательства $\neg\phi(\overline{\langle\langle\phi\rangle\rangle})$). Мы также можем выразить его в формальной арифметике аналогично ω_1 (обозначим выражающую формулу за ω_2).

Тогда рассмотрим формулу $\rho(x) \equiv \forall p(\omega_1(x,p) \to \exists q(q < p \& \omega_2(x,q)))$. Неформальным языком она утверждает, что для любого доказательства самоприменения некоторой формулы с номером a найдется доказательство (да еще и с меньшим гёделевым номером) отрицания этой формулы. Ну и по традиции применим ее к своему номеру r. Внимательное рассмотрение этой ситуации приводит к следующей теореме.

Теорема 12.4. Теорема Гёделя в форме Россера. Если формальная арифметика непротиворечива, то найдется такая формула ϕ, что как она сама, так и ее отрицание недоказуемы.

Докажем эту теорему, рассмотрев вспомогательную лемму:

Лемма 12.5. Каково бы ни было число n, доказуемы следующие утверждения:

- $\vdash a \le \overline{n} \to (a = \overline{0} \vee a = \overline{1} \vee \dots \vee a = \overline{n})$
- $\vdash (a = \overline{0} \vee a = \overline{1} \vee \dots \vee a = \overline{n}) \to a \le \overline{n}$

Доказательство. Импликации доказываются индукцией по n. Мы не будем предлагать подробного доказательства (в силу его размера и технического характера), наметим только несколько шагов. Доказательство значительно объемнее, но делается достаточно похоже.

Докажем первую импликацию. Рассмотрим индукцию по b на мета-языке.

База. $n = 0$. Тогда $a \le \overline{n}$ после подстановки b и раскрытия определения отношения «меньше» превращается в $\exists b(a + b = 0)$. Нам нужно показать, что $\vdash \exists b(a + b = 0) \to a = 0$

Утверждение может быть получено применением правила введения $\exists$ из более простого: $\vdash a + b = 0 \to a = 0$.

Докажем данное утверждение индукцией по b в предметном языке — применив схему аксиом индукции.

Рассмотрим сокращение записи: $A(b) \equiv a + b = 0 \to a = 0$ Тогда следующее выражение — аксиома (по схеме A9): $A(0) \& \forall b(A(b) \to A(b')) \to A(b)$. Если показать $A(0)$ и $\forall b(A(b) \to A(b'))$, то из этого по правилу M.P. будет нетрудно получить необходимое $A(b)$.

Покажем $A(0)$.

$(1..l)$	$a + 0 = 0 \to a + 0 = a \to a = 0$	Акс. A2 + переим.
$(l+1)$	$a + 0 = a \to a + 0 = 0 \to a + 0 = a$	Сх. акс. 1
$(l+2)$	$a + 0 = a$	Акс. A6
$(l+3)$	$a + 0 = 0 \to a + 0 = a$	M.P.
$(l+4..m)$	$a + 0 = 0 \to a = 0$	Сх. акс. 2 + M.P.

Теперь покажем $A(b) \to A(b')$.

(1)	$a + b' = (a + b)' \to a + b' = 0 \to (a + b)' = 0$	Сх. акс. 1
(2)	$a + b' = 0 \to (a + b)' = 0$	Акс. A5
$(3..k)$	$a + b' = 0 \to \neg(a + b)' = 0$	Акс. A4 + замена пер. + ослабление
$(k+1)$	$(a + b' = 0 \to (a + b)' = 0) \to$ $(a + b' = 0 \to \neg(a + b)' = 0) \to$ $(\neg a + b' = 0)$	
(l)	$\neg a + b' = 0$	M.P. 2 раза
$(l+1..m)$	$(a + b' = 0) \to (\neg a + b' = 0) \to (a = 0)$	Инт. сх. акс. 10
$(m+1..p)$	$(a + b' = 0) \to (a = 0)$	Сх. акс. 2 + M.P. 2 раза
$(p+1..q)$	$(a + b = 0 \to a = 0) \to (a + b' = 0 \to a = 0)$	Ослабление

□

Доказательство. Теперь приступим к теореме Геделя. В качестве формулы ϕ возьмем формулу $\rho(\overline{\text{«}\rho\text{»}})$.

Покажем недоказуемость ϕ. Пусть $\vdash \rho(\overline{\text{«}\rho\text{»}})$, т.е.

$\vdash \forall p(\omega_1(\overline{\text{«}\rho\text{»}}, p) \to \exists q(q < p \& \omega_2(\overline{\text{«}\rho\text{»}}, q)))$. У этого доказательства есть некоторый номер t, причем $\omega_1(\overline{\text{«}\rho\text{»}}, \bar{t})$. Несложно показать $\vdash (\omega_1(\overline{\text{«}\rho\text{»}}, \bar{t}) \to \exists q(q < \bar{t} \& \omega_2(\overline{\text{«}\rho\text{»}}, q)))$. По построению формулы $\vdash \omega_1(\overline{\text{«}\rho\text{»}}, \bar{t})$, откуда, соединив доказательства воедино, и применив правило Modus Ponens, получим $\vdash \exists q(q < \bar{t} \& \omega_2(\overline{\text{«}\rho\text{»}}, q)))$.

Так как теория непротиворечива, то не существует вывода формулы $\forall p(\omega_1(\overline{\text{«}\rho\text{»}}, p) \to \exists q(q < p \& \omega_2(\overline{\text{«}\rho\text{»}}, q)))$. Поэтому $W_2(\text{«}\rho\text{»}, q)$ ложно при любом q. Значит, по выразимости W_2, $\vdash \neg\omega_2(\overline{\text{«}\rho\text{»}}, q)$ для любого q, в том числе и для $q < t$. Отсюда можно показать, что $\vdash \neg\omega_2(\overline{\text{«}\rho\text{»}}, \bar{0}) \& \neg\omega_2(\overline{\text{«}\rho\text{»}}, \bar{1}) \& \ldots \& \neg\omega_2(\overline{\text{«}\rho\text{»}}, \overline{t-1})$ Применив лемму мы получаем, что $\forall q(q < \bar{t} \to \neg\omega_2(\overline{\text{«}\rho\text{»}}, q))$, от этого же можно перейти к $\neg\exists q(q < \bar{t} \& \omega_2(\overline{\text{«}\rho\text{»}}, q))$.

Обратно, пусть $\vdash \neg\phi$. Пусть t - гёделев номер доказательства. Раз так, то $W_2(\text{«}\rho\text{»}, t)$ истинно. По непротиворечивости формальной арифметики это значит, что $W_1(\text{«}\rho\text{»}, p)$ при любом p ложно (иначе окажется, что найдутся как доказательство, так и опровержение $\rho(\overline{\text{«}\rho\text{»}})$). Значит, доказуемо $\neg\omega_1(\overline{\text{«}\rho\text{»}}, \bar{p})$ при любом p (т.е. никакой из p не является доказательством $\rho(\overline{\text{«}\rho\text{»}})$). Как частный случай, $\neg\omega_1(\overline{\text{«}\rho\text{»}}, \bar{x})$ доказуемо для всех x, не превышающих t, поэтому $\vdash \neg\omega_1(\overline{\text{«}\rho\text{»}}, \bar{0}) \& \neg\omega_1(\overline{\text{«}\rho\text{»}}, \bar{1}) \& \ldots \& \neg\omega_1(\overline{\text{«}\rho\text{»}}, \bar{t})$. Отсюда можно показать $\vdash p \leq \bar{t} \to \neg\omega_1(\overline{\text{«}\rho\text{»}}, p)$.

Рассмотрим формулу $(p > \bar{t}) \to \exists q(q < p \& \omega_2(\overline{\text{«}\rho\text{»}}, q))$ Формула утверждает следующее: «если некоторый p больше t, то найдется такой q, меньший p, что $W_2(\text{«}\rho\text{»}, q)$». Очевидно, что данная формула истинна, ведь если мы возьмем t в качестве такого q, то $W_2(\text{«}\rho\text{»}, t)$ истинно по предположению. В силу выразимости W_2 в формальной арифметике формула также и доказуема.

Легко показать, что из этих утверждений и из того, что $p \leq \bar{t} \vee p > \bar{t}$, можно вывести $\neg\omega_1(\overline{\text{«}\rho\text{»}}, p) \vee \exists q(q < p \& \omega_2(\overline{\text{«}\rho\text{»}}, p))$, а отсюда - $\forall p(\omega_1(\overline{\text{«}\rho\text{»}}, p) \to \exists q(q < p \& \omega_2(\overline{\text{«}\rho\text{»}}, q)))$, то есть $\vdash \phi$. Однако, мы предположили $\vdash \neg\phi$, и исходя из него, вывели ϕ, т.е. показали противоречивость формальной арифметики. Значит, $\neg\phi$ также недоказуемо, если арифметика непротиворечива. □

Выберем утверждение, которое показывает непротиворечивость арифметики, т.е. показывает отсутствие такой формулы ϕ, что и ϕ и $\neg\phi$ доказуемы. Поскольку в противоречивой теории можно вывести любое утверждение, нам достаточно проверить это для какого-то конкретного ϕ, пусть это будет $1 = 0$. Ясно, что $\neg 1 = 0$ доказуемо. Тогда для доказательства непротиворечивости арифметики нам достаточно доказать $\forall p(\neg Proof(\overline{\text{«}1 = 0\text{»}}, p))$. Обозначим это утверждение за $Consis$.

Теорема 12.6. Вторая теорема Гёделя о неполноте арифметики. Если арифметика непротиворечива, то в ней не существует доказательства $Consis$.

Доказательство. Рассмотрим формулу $Consis \to \sigma(\overline{\text{«}\sigma\text{»}})$. Данная формула в точности соответствует условию первой части первой теоремы Гёделя о неполноте арифметики: если арифметика непротиворечива, то самоприменение формулы σ истинно, т.е. недоказуемо; напомним, что $\sigma(x) \equiv \forall p \neg\omega_1(x, p)$.

Рассуждение, доказывающее теорему Гёделя, можно формализовать, получив доказательство данной импликации. Теперь, если у нас будет доказательство утверждения $Consis$, то по правилу Modus Ponens мы также получаем доказательство утверждения $\sigma(\text{«}\sigma\text{»})$, что невозможно по первой теореме Гёделя. □

В данном месте есть очень поучительный пример, показывающий важность формализации, и существенность деталей, которые мы опустили в доказательстве второй теоремы о неполноте. В самом деле, вместо формулы $Consis$ мы могли бы попробовать рассмотреть

формулу $Proof1(a) := Proof(a,x)\&\neg(Proof(\text{«}1 = 0\text{»}, x))$ и построить по ней формулу $Consis1 := \forall x \neg Proof1(\text{«}1 = 0\text{»}, x)$ На первый взгляд, замена равноценна: действительно, если арифметика непротиворечива, то тогда $Proof1$ ничем не отличается от $Proof$, поскольку $1 = 0$ тогда действительно недоказуема. Если же арифметика противоречива, то $Consis1$ доказуема, как и любая другая формула.

Однако, $Consis1$ легко доказать. Пусть $\pi(x) \equiv Proof(\text{«}0 = 1\text{»}, x)$, тогда:

(1..n)	$\neg(\pi(x)\&\neg(\pi(x)))$	Доказуемо в и.в.
(n+1)	$\neg a = 0$	Аксиома A.x
(n+2)	$\neg(\pi(x)\&\neg(\pi(x))) \to \neg a = 0 \to \neg(\pi(x)\&\neg(\pi(x)))$	Сх. акс. 1
(n+3)	$\neg a = 0 \to \neg(\pi(x)\&\neg(\pi(x)))$	М.Р. n,$n+2$
(n+4)	$\neg a = 0 \to \forall x \neg(\pi(x)\&\neg(\pi(x)))$	Введение $\forall$ к $n+3$
(n+5)	$\forall x \neg(\pi(x)\&\neg\pi(x))$	М.Р. $n+1$, $n+4$

Получается, что мы здесь, продолжив рассуждение в соответствии со второй теоремой, можем сразу получить противоречие и показать противоречивость арифметики? На самом деле нет, поскольку мы некритично обобщили вторую теорему на случай формулы $Consis1$, тогда как она существенно использует внутреннее устройство $Consis$. У $Consis1$ ведь есть «слепое пятно» — формула $1 = 0$, на которой его результат не вычисляется, а постулируется, и это значительное отличие.

Чтобы абстрагироваться от конкретного вида $Consis$, Гильбертом и Бернайсом были предложены следующие условия выводимости, позволяющие считать, что формула действительно выражает непротиворечивость арифметики. Мы приведем их в более позднем варианте, сформулированном Лёфом.

Пусть $Consis \equiv \neg Provable(\text{«}1 = 0\text{»})$. Тогда $Provable$ должно отвечать следующим свойствам:

1. $\vdash \alpha$ влечет $\vdash Provable(\text{«}\alpha\text{»})$
2. $\vdash Provable(\text{«}\alpha\text{»}) \to Provable(\text{«}Provable(\text{«}\alpha\text{»})\text{»})$
3. $\vdash Provable(\text{«}\alpha \to \beta\text{»}) \to Provable(\text{«}\alpha\text{»}) \to Provable(\text{«}\beta\text{»})$

Заметим, что в случае $Provable1(a) = \exists x(Proof(a,x)\&\neg Proof(\text{«}1 = 0\text{»}, x))$ у нас будут сложности с демонстрацией третьего правила. Анализ таблицы истинности импликации (вместе с полнотой и.в.) указывает, что чтобы показать

$$\vdash Provable1(\text{«}2 = 0 \to 1 = 0\text{»}) \to Provable1(\text{«}2 = 0\text{»}) \to Provable1(\text{«}1 = 0\text{»})$$

нам надо показать $\vdash \neg Provable1(\text{«}2 = 0\text{»})$, поскольку $\vdash Provable1(\text{«}2 = 0 \to 1 = 0\text{»})$ и $\vdash \neg Provable1(\text{«}1 = 0\text{»})$. То есть, мы получим эту импликацию, только если покажем доказуемость непротиворечивости формальной арифметики (ведь $\vdash \neg Provable1(\text{«}2 = 0\text{»})$ — это тоже вариант $Consis$).

Если бы речь шла об обычной формуле $Provable$, мы бы решили вопрос следующим неформальным, но формализуемым доказательством: если существует x, такой, что $Proof(\text{«}2 = 0\text{»}, x)$, и существует y, что $Proof(\text{«}2 = 0 \to 1 = 0\text{»}, y)$, то выполнено и $Proof(\text{«}1 = 0\text{»}, x@y@\text{«}1 = 0\text{»})$.

В случае же с $Provable1$ нам все равно необходимо показывать $\vdash \neg Provable1(\text{«}1 = 0\text{»})$.

Мы можем, конечно, указать общее соображение: если бы было верно $Provable1(\text{«}2 = 0\text{»})$, то тогда было бы верно $\vdash 2 = 0$, значит, теория противоречива и найдется доказательство чего угодно, в том числе и $\vdash Provable1(\text{«}1 = 0\text{»})$, значит, выполнено $\neg Provable1(\text{«}2 = 0\text{»})$. Но это рассуждение касается только значений формулы $Provable1$, сформулировано на мета-языке, и непонятно, как из него сделать формальное доказательство $\vdash \neg Provable1(\text{«}2 = 0\text{»})$.

13 Теория множеств.

Теория множеств — это еще одна теория первого порядка, с которой мы познакомимся в этом курсе. Мы добавим к исчислению предикатов один новый двуместный предикат — отношение принадлежности $\in$.

Для изучения теории множеств мы введем несколько сокращений записи. Первое сокращение — это новая логическая связка *эквивалентность*.

Определение 13.1. Эквивалентность. Запись $a \leftrightarrow b$ является сокращением записи для $\equiv a \to b \& b \to a$.

Определение 13.2. Будем говорить, что множество x является подмножеством множества y, если любой элемент x принадлежит y. Формально: $x \subseteq y$ является сокращением записи для $\forall z(z \in x \to z \in y)$.

Определение 13.3. Принцип объемности.Два множества называются равными, если они являются подмножествами друг друга. Формально: $x = y$ является сокращением записи для $x \subseteq y \& y \subseteq x$.

Аксиома 13.1. Аксиома равенства. Равные множества содержатся в одних и тех же множествах. $\forall x \forall y \forall z(x = y \& x \in z \to y \in z)$.

Аксиома 13.2. Аксиома пары. Каковы бы ни были два различных множества x и y, существует множество, состоящее в точности из них. Будем записывать его так: $\{x, y\}$. Формально: $\forall x \forall y(\neg x = y \to \exists p(x \in p \& y \in p \& \forall z(z \in p \to (z = x \vee z = y))))$.

Аксиома 13.3. Аксиома объединения. Для любого множества x, содержащего хотя бы один элемент, найдется такое множество, которое состоит в точности из тех элементов, из которых состоят элементы x. Будем записывать его так: $\cup x$. Формально: $\forall x(\exists y y \in x \to \exists p \forall y(y \in p \leftrightarrow \exists s(y \in s \& s \in x)))$

Аксиома 13.4. Аксиома степени. Каково бы ни было множество x, существует множество 2^x, содержащее в точности все возможные подмножества множества x. Формально: $\forall x \exists p \forall y(y \subseteq p \leftrightarrow y \in x)$.

Аксиома 13.5. Схема аксиом выделения. Для любого множества x и любой формулы от одного аргумента $\phi(y)$, такой, что b в нее не входит свободно, найдется такое множество b, в которое входят те и только те элементы из множества x, что $\phi(y)$ истинно. Формально: $\forall x \exists b \forall y(y \in b \leftrightarrow (y \in x \& \phi(y)))$

Определение 13.4. Пересечением множеств x и y называется множество, состоящее в точности из тех элементов, которые присутствуют и в x и в y. Формально: $x \cap y$ — это такое множество z, что $\forall t(t \in z \leftrightarrow t \in x \& t \in y)$

Определение 13.5. Пустое множество $\emptyset$ — множество, которому не принадлежит никакой элемент: $\forall x \neg x \in \emptyset$.

Теорема 13.1.

1. Для любого множества X существует множество $\{X\}$, содержащее в точности X.
2. Если существует хотя бы одно множество, то существует пустое множество.
3. Пустое множество единственно.
4. Для двух множеств существует множество, являющееся их пересечением.

Определение 13.6. Дизъюнктным (разделённым) множеством называется множество, элементы которого не пересекаются. Формально:

$$Dj(x) \equiv \forall y \forall z((y \in x \& z \in x \& \neg y = z) \to \neg \exists t(t \in y \& t \in z))$$

Определение 13.7. Прямым произведением дизъюнктного множества a называется множество $\times a$ всех таких множеств b, что b пересекается с каждым из элементов множества a в точности в одном элементе.

$$\forall b(b \in \times a \leftrightarrow (\forall y(y \in a \to \exists! x(x \in y \& x \in b))))$$

Заметим, что прямое произведение дизъюнктного множества существует по аксиоме выделения, поскольку $\times a \subseteq \cup a$.

Аксиома 13.6. Аксиома выбора. Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто. Формально:

$$\forall t(Dj(t) \to \forall x(x \in t \to \exists p(p \in x)) \to \exists p(p \in \times t))$$

Аксиома 13.7. Аксиома бесконечности. Существует множество N, такое, что:

$$\emptyset \in N \& \forall x(x \in N \to x \cup \{x\} \in N)$$

Аксиома 13.8. Аксиома фундирования. В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x(x = \emptyset \vee \exists y(y \in x \& y \cap x = \emptyset))$$

Аксиома фундирования исключает множества, которые могут принадлежать сами себе (возможно, через цепочку принадлежностей): $X \in Y \in Z \in X$

Определение 13.8. Упорядоченная пара. Упорядоченной парой двух множеств a и b назовем множество $\{a, \{a, b\}\}$, еще будем записывать его так: $\langle a, b \rangle$

Лемма 13.2. Упорядоченную пару можно построить для любых множеств, также $\langle a, b \rangle = \langle c, d \rangle$ тогда и только тогда, когда $a = b$ и $c = d$.

Аксиома 13.9. Схема аксиом подстановки. Если задана некоторая функция f, представимая в исчислении предикатов (то есть, задана некоторая формула ϕ, такая, что $f(x) = y$ тогда и только тогда, когда $\phi(x, y) \& \exists! z \phi(x, z)$), то для любого множества S существует множество f(S) — образ множества S при отображении f.

Формально:

$$\forall s(\forall x \forall y_1 \forall y_2(x \in s \& \phi(x, y_1) \& \phi(x, y_2) \to y_1 = y_2) \to \exists t \forall y(y \in t \leftrightarrow \exists x(x \in s \& \phi(x, y))))$$

Через данную аксиому легко выразить аксиому выделения, однако аксиома подстановки не может быть сведена к аксиоме выделения.

Наличие аксиомы подстановки отличает аксиоматику Цермело-Френкеля от аксиоматики Цермело. Данная аксиома позволяет строить множества большой и очень большой мощности: допустим, если при $D(m) = 2^m$ положить $f(x) = D^x(\omega)$ (то есть $f(1) = 2^\omega$, $f(2) = 2^{2^\omega}$, ...), то мощность $\cup f(\omega)$ будет больше мощности любого кардинального числа с конечным номером. Впрочем, эта аксиома нужна даже для доказательства существования $2 \cdot \omega$: аксиома бесконечности гарантирует существование только ω.

Определение 13.9. Бинарное отношение Бинарным отношением на множестве X назовем подмножество множества всех упорядоченных пар элементов из X.

На бинарных отношениях естественным образом вводятся отношения рефлексивности, симметричтности и транзитивности.

Определение 13.10. Упорядочивание Отношение R на множестве S упорядочивает X, если это отношение транзитивно и оно образует линейный порядок (строгое неравенство: справедливо $\forall x \forall y(x \in X \to y \in X \to R(x,y) \vee x = y \vee R(y,x))$ и $\forall x \neg R(x,x)$). Отношение вполне упорядочивает S, если к тому же для любого непустого подмножества S выполнено $\exists x(x \in B \& \forall y(y \in B \to \neg R(y,x)))$.

Также можно ввести понятие максимума, минимума, верхней грани, супремума.

Определение 13.11. Множество x - транзитивное, если $z \in y, y \in x \to z \in x$.

Определение 13.12. Ординал (порядковое число) — транзитивное, вполне упорядоченное с помощью отношения $(\in)$ множество.

Рассмотрим ординалы подробнее. Для начала рассмотрим *конечные* ординалы: $0 := \emptyset$; $1 := \{\emptyset\}$; $2 := 1 \cup \{1\}$ и т.п. Существование каждого из этих ординалов легко доказать.

Определение 13.13. Ординал x называется предельным, если $\neg x = \emptyset \& \neg \exists y(y \cup \{y\} = x)$.

Минимальный предельный ординал мы обозначим ω. Ясно, что любое натуральное число меньше, чем ω. Также легко заметить, что ω содержит в себе в точности все конечные ординалы.

Для ординалов можно определить арифметические операции. В силу ограниченности курса мы сделаем это неформально, на мета-языке.

Определение 13.14. Арифметические операции над ординалами. За $a + 1$ обозначим $x \cup \{x\}$. Тогда следующими рекурсивными определениями мы введем операции сложения, умножения и возведения в степень:

$$a + b \equiv \begin{cases} a, & b \equiv 0 \\ (a + c) + 1, & b \equiv c + 1 \\ sup\{a + c | c < b\}, & b \text{ — предельный ординал} \end{cases}$$

$$a \cdot b \equiv \begin{cases} 0, & b \equiv 0 \\ (a \cdot c) + a, & b \equiv c + 1 \\ sup\{a \cdot c | c < b\}, & b \text{ — предельный ординал} \end{cases}$$

$$a^b \equiv \begin{cases} 1, & b \equiv 0 \& a > 0 \\ (a^c) \cdot a, & b \equiv c + 1 \\ sup\{a^c | c < b\}, & b \text{ — предельный ординал} \end{cases}$$

Заметим, что в смысле введенной операции прибавления единицы, предельный ординал — это такой ненулевой ординал x, для которого нет ни одного ординала y, что $y + 1 = x$.

Так определенные операции на конечных ординальных числах ведут себя подобно обычным арифметическим операциям на натуральных числах, однако в целом их поведение может быть неочевидным. Например, легко заметить, что $1 + \omega = \omega$.

Определение 13.15. Назовем множества X и Y равномощными, если найдется биективное отображение X на Y. Будем записывать это как $|X| = |Y|$. Будем говорить, что множество X имеет мощность не превышающую Y, если найдется инъективное отображение X в Y. Будем записывать это как $|X| \leq |Y|$. Будем записывать $|X| < |Y|$, если известно, что $|X| \leq |Y|$, но неверно, что $|X| = |Y|$.

Определение 13.16. Кардинальные числа Кардинальное число - такой ординал x, что $y < x \leftrightarrow |y| < |x|$.

Ясно, что все конечные ординальные числа являются кардинальными. Также, например ω — кардинальное число (еще оно обозначается как $\aleph_0$, если речь идет о мощности множеств). 2^ω — кардинальное число $\aleph_1$, соответствует мощности континуум.

Есть ли какое-нибудь кардинальное число между $\aleph_0$ и $\aleph_1$? Континуум-гипотеза (что никаких других кардинальных чисел между ними нет) была высказана довольно давно, и длительное время была одной из главных проблем в теории множеств. Сначала Геделем было показано, что континуум-гипотеза не противоречит ZF. Утверждение о том, что и отрицание континуум-гипотезы не противоречит ZF, было доказано через 30 лет Коэном.

14 Теорема Лёвенгейма-Сколема

Как мы знаем из предыдущих разделов, рассмотрение формальной теории неполно, если не сопровождается рассмотрением её моделей. Действительно, каковы могут быть модели теории множеств? Например, обязан ли объект, соответствующий множеству мощности $\aleph_1$ действительно иметь несчётное количество элементов? В данном разделе мы прольём некоторый свет на этот вопрос.

Определение 14.1. Мощность модели. Пусть M — модель некоторой теории первого порядка. Напомним, что модель задаётся предметным множеством D, и функциями, соответствующим всем предикатам теории и всем функциональным символам теории. Тогда, назовем мощность множества D мощностью модели.

Определение 14.2. Элементарная подмодель. Пусть M — модель некоторой теории первого порядка, с предметным множеством D, и пусть определено D_1, $D_1 \subset D$. Тогда структура M_1, построенная на предметном множестве D_1 с предикатами и функциями, получающимися из предикатов и функций M путем сужения их области определения на D_1 называется *элементарной подмоделью* M, если:

1. любая функция теории f замкнута на D_1 (т.е. если $x_1 \in D_1, \dots x_n \in D_1$, то $f(x_1, \dots x_n) \in D_1$)
2. любая формула $A(x_1, \dots x_n)$ теории при любых значениях $x_1, \dots x_n$ из D_1 истинна в M_1 тогда и только тогда, когда она истинна в M.

Заметим, что второе условие необходимо: пусть некоторая теория 1го порядка содержит предикат равенства. Тогда формула $\exists x \exists y \neg(x = y)$ при сужении предметного множества до одноэлементного перестаёт быть верной.

Лемма 14.1. Элементарная подмодель теории является моделью данной теории.

Доказательство. Рассмотрим некоторую доказуемую формулу теории A. Она является общезначимой в M, значит, она является общезначимой в M_1. □

Определение 14.3. Назовём теорию счётно-аксиоматизируемой (конечно-аксиоматизируемой), если ее множество аксиом и правил вывода имеет счётную (конечную) мощность.

Заметим, что аксиомы и правила вывода явно содержат все «содержательные» формулы в теории — формулы, которые могут использоваться в доказательствах хоть в каком-нибудь качестве. В наших определениях ничего не запрещает создать теорию, в которой заданы и дополнительные функции и предикаты, ни разу не упоминаемые в аксиомах и

правилах вывода, но таким предикатам и функциям мы можем приписать произвольный смысл (например, все функции возвращают некоторую заранее выбранную константу c_0, а все предикаты ложны), не повредив корректности модели. Поэтому мы без ущерба для общности можем предположить, что язык теории не содержит «несодержательных» формул. При этом заметим, что в силу конечного размера каждой аксиомы и правила вывода любая конечно(счётно)-аксиоматизируемая теория имеет конечное (счётное) множество всех возможных «содержательных» формул.

Теорема 14.2. Теорема Лёвенгейма-Сколема. Пусть M — модель некоторой теории первого порядка, и пусть T — множество всех формул этой теории. Тогда у M есть элементарная подмодель, такая, что $|M| = max(|T|, \aleph_0)$.

Доказательство. Для построения требуемой модели нам необходимо построить предметное множество требуемой мощности и показать, что сужение теории на него даст нам элементарную подмодель. Отсюда доказательство естественным образом разбивается на две части.

Часть 1. Построение множества. Рассмотрим некоторое предметное множество D'. На его основе построим множество D'', рассмотрев все формулы из T, и по каждой формуле (возможно) добавив некоторое количество элементов к D'.

Фиксируем некоторую n-местную формулу $A(y, x_1, \dots x_n)$ из T. Фиксируем некоторый набор аргументов $x_1, \dots x_n$ из D'. В ходе вычисления A в результате применения функций к аргументам мы можем выйти из D' — добавим эти новые константы к D''. Их будет не более чем конечное количество. Заметим, что формула A может быть:

- тождественно истинной или ложной при любом y из D — пропустим эту формулу и пойдем дальше. Поступим так же, если функция может быть как истинной так и ложной при разных значениях y из D'.
- Найдутся такие y, что $A(y, x_1, \dots x_n)$ истинна, но при этом для любого y из D' формула $A(y, x_1, \dots x_n)$ ложна — тогда добавим какой-нибудь один из этих y к множеству D''. Также пополним множество всеми константами, которые необходимо добавить вследствие вычисления A на данных аргументах. Этим мы также увеличим D'' на конечное количество элементов.

Рассмотрим множество D_0, $D_0 \subseteq D$, такое, что в него входят только те элементы предметного множества, которые соответствуют константам (т.е. нуль-местным функциям), упоминающимся в формулах из T. Если это множество получается пустым — добавим к нему какую-нибудь одну константу из D. Оно ляжет в начало счётной последовательности из множеств, $D_0 \subseteq D_1 \subseteq D_2 \subseteq \dots$ (такой, что $D'_k = D_{k+1}$), объединив которую, мы получим множество D^*, которое и будет требуемым предметным множеством.

Заметим, что в результате однократного процесса пополнения мы увеличим множество D' не более чем на $|T| \cdot \aleph_0 \cdot |D'|$ элементов (по каждой формуле по каждой константе из D' добавим не более, чем конечное количество элементов). Поэтому мы не выйдем из мощности $|T|$, если T несчётно, или из $\aleph_0$, если T — конечно. Значит, мощность D^* также будет отвечать условию теоремы.

Часть 2. Покажем, что структура M^*, полученная сужением модели M на предметное множество D^*, является элементарной подмоделью. Докажем это индукцией по структуре формул. Рассмотрим некоторую формулу $A(x_1, \dots x_n)$, при этом $x_i \in D^*$.

База. Эта формула — предикат $P(f_1(x_1, \dots x_n), \dots f_k(x_1, \dots x_n))$. Если $x_1, \dots x_n$ взяты из D^*, то все они добавлены на некотором шаге, значит, найдётся такой t, что $x_i \in D_t$. Значит, все результаты функций $f_j(x_1, \dots x_n)$ лежат в D_{t+1}. Значит, формула будет определена на этих значениях. Очевидно, что истинность (ложность) формулы сохранится.

Переход. Пусть есть некоторая формула A — связка одной или двух подформул, и A имеет следующий вид:

1. $X\&Y, X \vee Y, \neg X, X \to Y$ — ясно, что все эти правила работают на сужении исходной модели, и истинность формулы сохраняется.

2. $\exists y B(y, x_1, \dots x_n)$. Фиксируем некоторый набор $x_1, \dots x_n$ из D^*. Пусть формула A истинна в M, покажем её истинность в M^*. Заметим, что каждый из x_i был добавлен в D^* на конкретном шаге, то есть найдется такой номер t, что все x_i принадлежат D_t. Тогда, по построению множества D_{t+1}, в нём неизбежно найдётся такой y, что $B(y, x_1, \dots x_n)$ определено и выполнено в M. Значит, B будет выполнено и в M^* (по предположению индукции). Значит, A истинна и в M^*. Обратное также очевидно: если y найдётся в узкой модели, то он тем более найдётся в широкой.

3. $\forall y B(y, x_1, \dots x_n)$. Доказательство зеркально соответствует предыдущему пункту. Истинность $\forall y B(y, x_1, \dots x_n)$ в M очевидно влечет истинность $\forall y B(y, x_1, \dots x_n)$ в M^*, так как $D^* \subseteq D$. Если же $\forall y B(y, x_1, \dots x_n)$ ложно в M, то существует такой y из D, что $\neg B(y, x_1, \dots x_n)$ истинно в M, значит, по построению D^* и в нём найдется элемент z с таким свойством, то есть $B(z, x_1, \dots x_n)$ ложно в M. И по предположению индукции $B(z, x_1, \dots x_n)$ ложно в M^*. То есть $\forall y B(y, x_1, \dots x_n)$ ложно в M^*.

□

Данная теорема в частности показывает, что для теории множеств (очевидно, счётно-аксиоматизируемой) имеется счётная модель. В частности, это приводит к следующему утверждению, называемому *парадоксом Сколема*: для любого множества, определимого в аксиоматике Цермело-Френкеля, мы можем предложить способ перенумеровать его элементы натуральными числами. В том числе это справедливо и для несчётных множеств — то есть для тех множеств, для которых доказано отсутствие этого способа.

Парадокс, тем не менее, здесь кажущийся, поскольку тут (некорректно) сталкивается утверждение, формулируемое на предметном языке (об отсутствии способа пересчёта внутри теории), с утверждением на мета-языке (о существовании этого способа вне теории).

15 Литература

Список литературы

[1] С. Клини. Математическая логика — М.: Изд-во «Мир», 1973

[2] Н.К. Верещагин, А. Шень, Лекции по математической логике и теории алгоритмов, Языки и исчисления — МЦНМО, 2002. Также доступно по ссылке `http://www.mccme.ru/free-books/shen/shen-logic-part2.pdf`

[3] Н.К. Верещагин, А. Шень, Лекции по математической логике и теории алгоритмов, Вычислимые функции — МЦНМО, 2002. Также доступно по ссылке `http://www.mccme.ru/free-books/shen/shen-logic-part3.pdf`

[4] Э. Мендельсон. Введение в математическую логику — М.: Изд-во «Наука», 1971.

[5] С. Клини. Введение в метаматематику — М.: Изд-во «Иностранная литература», 1957.

[6] Makoto Kikuchi. Kolmogorov complexity and the second incompleteness theorem. Arch. Math. Logic 36: 437-443 (1997)

[7] Shira Kritchman, Ran Raz. The Surprise Examination Paradox and the Second Incompleteness Theorem. Notices of the AMS volume 57(11): 1454-1458 (2010)

[8] А.А. Френкель, И. Бар-Хиллел. Основания теории множеств — М.: Изд-во «Мир», 1966.

[9] П.Дж. Коэн. Теория множеств и континуум-гипотеза — М.: Изд-во «Мир», 1969.